UNIVERSITY OF DERBY

(Mis)Use of Personal Technology by Employees in Financial Services Organisations

Raichel Collis

A submission in partial fulfilment of the requirements of the University of Derby for the award of the degree of Doctor of Philosophy.

College of Business, Law and Social Sciences

March 2021

Contents

Figures, Tables and Legislation……xiv

Glossary of Acronyms and Nomenclature……..……...xvii

.

Preface……..…….xx

Abstract…….……xxi

Acknowledgements……xxii

Chapter One: Introduction

1.1 Introduction to Personal Technologies……..1

1.2 The Central Investigation and Research Questions…….....3

1.3 Theoretical Frameworks……...…...5

1.4 Original Contribution…….……..5

1.5 Thesis Arrangement……..……....6

1.6 Additional Resources for the Reader…..……....10

Chapter Two: 'The Theoretical Framework for RAT in Cyberspace'

2.1 Introduction…….……12

2.2 A Brief Introduction to Routine Activity Theory…….……...13

2.3 The Internet for All……..……..16

2.3.1 Routine Cyber Activity…..……..18

2.3.2 Digital Footprints: Passive Footprints……...…….....19

2.3.3 Digital Footprints: Active Footprints…….……...20

2.3.4 User Augmentation…..…….…23

2.3.5 Impact of Digital Footprints…..……..……..25

2.3.6 Erasing Data…..…….…25

2.3.7 Active and Passive Data as Intelligence Tools…..……..……26

2.4 Routine Activity Theory in the Cyber Domain…...…….……...27

2.4.1 Time and Space in the Virtual World…...…..…….……28

2.5 Cyberspace is Different!.....30

2.5.1 Physical RAT and Cyber-RAT – not so different after all?.....30

2.5.2 Target Attractiveness…….…….……..34

2.5.3 Capable Guardians in Cyberspace…..…….……...38

2.5.4 The Networked Society as Guardians…..…….……....39

2.5.5 Observed Guardianship…..…...……..…..41

2.6 The Average User…..…….…….……...43

2.6.1 The User as Capable Guardian…..…….44

2.7 Cyber-RAT in Action…...…….…..….47

2.7.1 Fluidity…...…….……..…….48

2.7.1.1 Physical and Virtual Offenders…..……..……..…….49

2.7.2 Fluidity and Liquid Modernity…..……..……..…….50

2.7.3 Control…..…….……...…..……53

2.7.4 A Theoretical Cyber-RAT Framework?.....…..…….…….54

2.8 Conclusion to the Theoretical Framework for RAT in Cyberspace……..…..55

Chapter Three: Literature Review

3.1 Introduction…….……58

3.1.1 Chapter Arrangement…..……..……....59

3.2 Cyber Threat to the Financial Sector…..…….....60

3.2.1 Perceived Insider Threat…..…….…….....62

3.3 The Internet…...…….……64

3.3.1 Internet Criminals…...…….…….....65

3.3.2 Vulnerabilities and Malware…….……66

3.4 Web 2.0 Technology…..……..…….……..71

3.4.1 Social Engineering…...…….……..…73

3.4.2 Phishing and Targeted Attacks…...……..74

3.4.3 Social Media and Frauds, Spam, Hoaxes, and Malware…...…….....76

3.5 Cloud Services…...……..……..…78

3.6 Summary of 3.3 to 3.5 in Relation to Research Questions 1 and 2…….....81

3.7 Mobile Internet Access……...……..……84

3.7.1 Mobile Operating Systems: Android and Apple…….……85

3.7.2 Vulnerabilities and Malware for Mobile Systems…...……..…….86

3.7.3 Mobile Device Security……..……89

3.7.4 Bring Your Own Device……..91

3.8 Summary of 3.7 in Relation to Research Questions 1 and 2……..……..93

3.9 Insider Threat: A New Perspective……...……..95

3.9.1 Too Many Threats – Not Enough Awareness…….……96

3.9.2 Employees and Corporate Systems…….……98

3.9.3 Bring Your Own Multiple Devices……...100

3.9.4 Social Media and Mobile Social Networking…...……..……103

3.9.5 Employees: Generational Differences…….……106

3.9.6 Shadow Systems: Shadow IT…….……..107

3.10 Summary of Relevance to the Research Questions……..……110

3.11 The Internet of Things (IoT)…….112

3.11.1 Smart Technology…….112

3.11.2 Consumer IoT…….114

3.11.3 Wearable Devices…….116

3.11.4 IoT Security Risks…….119

3.11.5 Shadow Systems: Shadow Internet of Things…….126

3.12 Summary of 3.11 in Relation to Research Question 3…….128

3.13 Analysis of the Literature Review…….129

3.14 Conclusion to the Literature Review…….131

Chapter Four: 'The Corporate World'
(Methodology One)

4.1 Introduction to the Methodologies..…….134

4.2 A Technological Research Strategy – In Theory..……..135

4.3 Positionality and Reflexivity..……138

4.3.1 The Human Phenomenon..……...139

4.3.2 Ontology in Design Practice..……140

4.3.3 A Design Epistemology..……141

4.3.4 Open-Source Research and Philosophical Frameworks..……142

4.3.5 Subjectivity and Bias.....……143

4.3.6 Ethics and Internet Research..……145

4.3.7 Three Methodologies for Digital Investigation..……...146

4.4 The Research Strategy – in Practice…….147

4.5 The Financial Industry: A Brief Overview…….....148

4.6 Web 2.0 as a Resource for Open-Source Intelligence……..150

4.6.1 Social Media Users as Assets for Academic Research……..152

4.7 Safeguarding Preparation for Online Research…….154

4.7.1 IP Addresses…….154

4.7.2 Footprints and Fake Identities……155

4.7.3 Social Media……..156

4.8 Preliminary Steps…….....157

4.8.1 Financial Organisations……..159

4.8.2 Professional Bodies and Industry Databases…..……159

4.8.3 Dating Sites……..160

4.8.3.1 Reflection on Dating Sites..……162

4.8.4 Keywords and Site or Domain Searching……..162

4.8.5 Instagram……...163

4.8.6 Real Time Social Search Engine…….....164

4.9 The List of Potential Candidates..……....165

4.9.1 Potential Candidates and LinkedIn..…….....165

4.9.2 OSINT Techniques..…….....168

4.10 Reflection..……169

4.11 Conclusion to ‘The Corporate World..…….....172

Chapter Five: ‘Executive Risk’
(Methodology Two)

5.1 Introduction……174

5.2 The Research Instrument…….……174

5.2.1 The Electronic Survey…….175

5.3 A New Approach for the Practical Research……..……..176

5.3.1 Open Sources……..……177

5.3.2 The LinkedIn Account……..……178

5.3.3 Searching for Executives……180

5.3.4 An Exploratory Search……180

5.3.5 The Search Parameters……..……181

5.4 The Practical Investigation……...……..183

5.4.1 Search Strategy: Photographs……..……184

5.4.2 Search Strategy: Social Media……..……..185

5.4.3 Search Strategy: Recognised User Behaviour……..……...186

5.4.4 Search Strategy: Heritage Data……..……188

5.5. The Business Report……..……190

5.5.1 Chief Information Security Officers……192

5.5.2 The Outcome……193

5.5.3 Inadvertent Social Engineering……..……194

5.6 Conclusion to ‘Executive Risk’……..……195

Chapter Six: ‘A New Direction’
(Methodology Three)

6.1 Recapitulation of the Outcome of ‘Executive Risk’...……..199

6.1.1 Introduction to ‘A New Direction’……200

6.2 Segment One: New Methods..…….....200

6.3 The Change to UK Data Protection Law: GDPR 2018..……203

6.4 The Letter of Introduction.……204

6.4.1 The ‘follow-up’ Email……205

6.4.1.1 Personal Email Addresses..……...206

6.4.1.2 Generic Email Addresses……..207

6.5 Invitations……207

6.5.1 Data Storage..……...208

6.6 Segment Two: Final Methods……...209

6.6.1 Professional and Industry Bodies..…….209

6.6.2 Financial Conferences and Training Events…….211

6.6.3 Contacts…….211

6.6.3.1 Academic……..212

6.6.3.2 Professional……..212

6.6.3.3 Industry 1……..213

6.6.3.4 Industry 2……..213

6.6.4 Personal Contacts……214

6.6.5 Regulatory Bodies……214

6.7 The Survey……...215

6.7.1 Data Cleansing……215

6.7.2 Restricted Questions……...217

6.7.3 The summary Report...……218

6.7.4 Mistakes in Logic and Piping……...221

6.8 Conclusion to ‘A New Direction’……..……..223

Chapter Seven: Recording the Data and Content Analysis

7.1 Introduction..……225

7.2 The Respondents……225

7.2.1 Gender and Age..…….226

7.2.2 Nationality……227

7.2.3 Education……227

7.2.4 Employment……228

7.2.5 Participating Organisations……229

7.2.6 Occupation……230

7.3 Personal Technologies……231

7.3.1 Personal Mobile Devices……231

7.3.2 Personal Internet Activity……233

7.3.3 Mobile Devices and Internet Activity……234

7.3.4 Mobile Devices in the Workplace……234

7.3.5 Work Activity using Personal Mobile Devices……235

7.4 A Brief Evaluation of Routine Activity using Applications……236

7.4.1 Streaming……238

7.4.2 The Significance of Access to Copyright Protected Material……240

7.4.3 Games……241

7.4.4 Games Malware……242

7.4.5 Gambling, Dating and ‘Adult’ Applications……243

7.4.6 Social Media……244

7.4.7 Communication Apps……245

7.5 The Central Research Questions……245

7.5.1 Apps Installed to a Personal Device……246

7.5.2 Outdated Apps……247

7.6 Mobile Device Security……248

7.6.1 Update When Prompted……249

7.6.2 Antivirus……250

7.6.3 iOS Users and Antivirus Solutions……..251

7.6.4 Users of Other Operating Systems and Antivirus Solutions……252

7.6.5 iOS and other Operating Systems in relation to RQ1 and RQ2.....254

7.7 Conclusion to Recording the Data and Content Analysis…..……255

Chapter Eight: Content Analysis and Interpretation

8.1 Introduction..……256

8.2 Digital Activity in the Workplace..……..257

8.2.1 Types of Company Issued Devices.……....259

8.2.2 Workplace Activity..……259

8.2.3 Software Updates and Downloading Apps..……261

8.2.4 Use of Apps Groups A and B: Organisations and Occupations..…..263

8.2.5 Groups A and B: Occupations Senior Personnel.……263

8.2.6 High-Level Personnel and Workplace Digital Activity..……264

8.2.7 Summary of Groups A and B in Relation to RQ1..……...266

8.3. Group C. Personal Devices..……...266

8.3.1 Routine Internet Activity in the User's Private Space..……267

8.3.2 Group C: Digital Activity Whilst Connected..……269

8.3.3 Group C: Occupations..……...271

8.3.4 Summary of Group C in Relation to RQ1 and RQ2..……272

8.4 A Further Exploration of Devices Connected to the Network...……274

8.4.1 Group C: Device Security – Updates...……274

8.4.2 Device Security and Digital Activity...……275

8.4.3 Number of Apps on Devices Connected to the Network...……276

8.4.4 Summary of Apps and Security in Relation to RQ1 and RQ2..……...279

8.5 The Most Popular ‘Unsafe’ Activities..……..280

8.5.1 Social Networks..……...280

8.5.2 Profiles..……281

8.5.3 Social Media Habits..……282

8.5.4 Privacy Controls..……283

8.5.5 Work Colleagues as Social Media Friends..……....284

8.5.6 Frequency of Posting Content on Social Media..……284

8.5.7 Social Media in the Corporate Workplace..……...286

8.5.8 Summary of Social Media in Relation to RQ1and RQ2...……287

8.6 Communication Apps...……289

8.6.1 Routine Use of Communication Apps in Personal Space...……290

8.6.2 Quantity of Communications Apps on Devices...……290

8.6.3 Popular Apps...……291

8.6.4 Communication Apps used in the Workplace……...292

8.6.5 Summary of Communication Apps in Relation to RQ1 & RQ2……293

8.7 The Internet of Things (RQ3).....……295

8.7.1 Employee IoT..……..297

8.7.2 Category of IoT..……...297

8.7.3 Quantity of IoT Units Owned by Employees...……..298

8.7.4 IoT Combinations...……..300

8.7.5 Device Security..……...300

8.7.6 Updates to IoT Devices...……302

8.7.7 Default Passwords..……304

8.8 Consumer IoT in the Workplace..……..305

8.8.1 Wearable Devices...……305

8.8.2 Wearable Devices Connected to the Network..……306

8.8.3 IoT Applications on a Device Connected to the Network..……..307

8.8.4 IoT Accessed from the Workplace..……309

8.8.5 Connecting to an Alternate Network..……....310

8.8.6 Summary of IoT in Relation to Research Question 3…...…….....312

8.9 Conclusion to Analysis and Interpretation…..……314

Chapter Nine: Discussion

9.1 Introduction..……316

9.2 Limitations in the Research Instrument and the Survey Process..……317

9.2.1 Respondent Error..……...317

9.2.2 The Five-Point Scales...……..318

9.2.3 Passed and Unanswered Questions……..319

9.2.3.1 Accidental or Deliberate..……..319

9.2.3.2 Anonymity……321

9.3 The Findings..……..321

9.3.1 Apps..……321

9.3.2 Communication Apps..……323

9.3.3 Absent Data..……324

9.3.4 Streaming and Piracy..……325

9.3.5 Absent Data Affecting the Value of the Findings..……328

9.3.6 Security Risks of Applications: Outdated Software……..330

9.3.7 Security Risks of Applications: Updates...…….331

9.4 Social Media..……..334

9.4.1 Oblivious Social Networking..…….335

9.4.2 Work Colleagues as Social Media Friends..…….336

9.4.3 User-Content about Children as an Aid to Attackers..……....337

9.4.4 Legacy Content...…….338

9.4.5 The ‘Narcissistic’ Social Media User…….340

9.5 Recommendations to Enhance Bespoke Training...……..341

9.5.1 Applications Intelligence...……..343

9.5.2 Enhanced Security...……345

9.5.3 iOS Users as a Challenge to Security..……..346

9.6 The Cyber-RAT Framework in Action..……..349

9.6.1 Routine Digital Activity..……...349

9.6.2 Cyber-RAT and Bespoke Training..……...351

9.6.3 Cyber-RAT and Threat Intelligence..…….354

9.7 Augmenting the Traditional Model of Insider Threat..…….....355

9.7.1 Personal Digital Activity using Company Issued Devices..…….356

9.7.2 High-Ranking Personnel and Executive Privilege..……....357

9.7.3 Enabled Guardianship as Risk..…….359

9.8 The Internet of Things (RQ3)..……....361

9.9 Conclusion to Discussion.……368

Chapter Ten: Conclusion

10.1 Introduction…….370

10.2 The Findings..……371

10.2.1 Research Question One.……..372

10.2.2 Research Question Two..……375

10.2.3 Research Question Three..……..377

10.2.4 Implications..……..379

10.3 Contribution to Knowledge..……380

10.4 Limitations……..387

10.5 Further Research..……388

10.6 Final Conclusion……391

References.……393

Appendix A: Erasing Digital Footprints from the Internet……..……..494

Appendix B: Digital Investigation for Financial Sector Executives……...497

Appendix C: Report Sent to Financial Organisations..……526

Appendix D: Impact of the Change in UK Data Protection Legislation.……...535

Appendix E: Letter of Invitation…….541

Appendix F: LinkedIn and Social Engineering..……..542

Appendix G: Guest Networks..……548

Appendix H: Cyber Awareness – Password Management……...551

Appendix I: The NHS Cyber Attack…….553

Confirmation of Ethical Approval……..555

Request for Ethical Approval……556

Figures, Tables and Legislation

Figure 1. Filter Question PQ5……219
Figure 2. Logic and Piped Answers Operating Correctly……220
Figure 3. Mistakes in Logic and Piped Answers..……...221
Figure 4. Respondent Age……226
Figure 5. Age and Gender……226
Figure 6. Nationality……227
Figure 7. Education..……..227
Figure 8. Occupation..……230
Figure 9. Personal Mobile Devices..……231
Figure 10. Quantity of Owned Personal Devices...……...232
Figure 11. Personal Internet Activity..……233
Figure 12. Primary Device used for Internet Activity……234
Figure 13. Type of Devices Taken to the Workplace……...235
Figure 14. Quantity of Devices Taken to the Workplace…….....235
Figure 15. Devices used for Work Activity..……..236
Figure 16. Routine Activity using Applications..……...237
Figure 17. Number of Apps on Devices……..246
Figure 18. Delete Apps or Software……...248
Figure 19. Update Device or Software When Prompted……..249
Figure 20. Antivirus Solutions on Personal Devices……250
Figure 21. Number of Respondents in Groups A, B and C…….....258
Figure 22. Company Issued Devices used for Digital Activity..…….....259
Figure 23. Workplace Activity using Company Devices...……...260
Figure 24. Company Issued and Personal Devices……..260
Figure 25. Occupations of Groups A and B..……....264
Figure 26. Senior Staff from Groups A and B using company devices..……...265
Figure 27. Group C: Routine Digital Activity in Personal Space……..268
Figure 28. Group C: Digital Activity whilst Connected to the Network.……...269
Figure 29. Group C: Occupations..……271
Figure 30. Social Media Profiles……...……....281
Figure 31. Using Devices for Social Media at Work…….....286
Figure 32. Routine Use of Communication Apps in Personal Space..……290

Figure 33. Quantity of Communication Apps on Devices..……....291
Figure 34. Popular Communication Apps..……...292
Figure 35. Communication Apps used in the Workplace..……...293
Figure 36. Employee IoT..…….....297
Figure 37. Category of IoT..……....298
Figure 38. Quantity of IoT..……..299
Figure 39. Security Research Prior to Purchase..……....301
Figure 40. Reasons for No Security Research..……301
Figure 41. Install IoT Updates..……..302
Figure 42. Default Password Changed When Device Installed..……...304
Figure 43. Devices Which May Retain Default Passwords..……..304
Figure 44. IoT Worn in The Workplace..……....306
Figure 45. Wearables Connected to the Network..……..306
Figure 46. IoT Apps on Connected Devices..……...308
Figure 47. Type of Data on a LinkedIn Profile……..……543
Figure 48. Personal Information on a LinkedIn Profile..……...544
Figure 49. Passwords……...551

List of Tables

Table 1. Active and Passive Digital Footprints……....22
Table 2. The Theoretical Cyber-RAT Framework..……54
Table 3. The Search for Financial Executives..……190
Table 4. Invitations to Participate……..……208
Table 5. Survey Submissions..……216
Table 6. Financial Services ……..…….....228
Table 7. Dates and Times of Survey Completion……..229
Table 8. iOS Users Comments regarding Antivirus ……251
Table 9. Users of Other Operating Systems regarding Antivirus……253
Table 10. Number of Apps on Devices Connected to the Network……..274
Table 11. Update of Apps and Operating Systems……275
Table 12. Group C. Irregular Updates and Digital Activity……..277
Table 13. Routine Activity with Limited Guardianship……280
Table 14. Respondents and Routine Social Media Activities……282

Table 15. Enabled Privacy Controls..……..283
Table 16. Work Colleagues as Friends and Followers..…….284
Table 17. Social Media Content and Frequency of Posts……..285
Table 18. Combinations of Consumer IoT..…….300
Table 19. IoT Accessed in the Workplace……...309
Table 20. Percentage of Respondents using Apps for 'Unsafe' Activity……..322

List of Legislation

UK Legislation

Data Protection Act 1998
Data Protection Act 2018
General Data Protection Regulation (GDPR)

EU Legislation

Data Protection Directive 95/46/EC

Glossary of Acronyms and Nomenclature

Blog	Originally 'weblog', a regularly updated online account written by a single user or organisation. Can be personal content or factual.
Cookie	A small piece of data sent from a website to a user's web browser. Intended to improve the browsing experience (Kaspersky, 2021).
Copyright Protected Content	Intellectual property with a legal right of ownership which should not be sold, shared, or copied without the owner's permission (EUIPO, 2018).
Cyberlocker	Online storage where users store and share files.
Dark Web	A 'hidden' part of the internet containing illicit websites, communities and marketplaces which cannot be accessed using normative search methods.
Encryption	The process of converting stored or in transit data into code to avoid unauthorised access (Rouse, 2020).
Exploit Kit	A type of 'cybercrime toolkit' consisting of a variety of exploits to target popular software packages, a console to manage the attack and add-on features to aid the attacker (TrendMicro, 2020).
Firewall Device	A hardware device or piece of software (or both) providing different levels of protection to a network.
Instagram	A social network where users share multi-media content and attach hashtags so that content can be categorised. Users can search using hashtags to find other content sharing the same tags.
IP (Internet Protocol) **Address**	A unique identifier assigned to each device accessing a network. Used as an 'address' to send data to specific devices connected to the internet (Pollette and Crawford, 2020).
LinkedIn	A social network designed for professionals who use the site for business networking, job search or personal promotion.
Malware	Malicious Software designed to infect a digital system and cause harm.
Netiquette	Standards of online behaviour showing respect to other users.
Payload	The part of an attack intended to cause harm (Cloudflare, 2020).

Pinterest	A social network where users collect visual images and media found throughout the internet and curate them into collections ‘pinned’ onto virtual notice ‘boards’.
Polymorphic Malware	Malware engineered to constantly alter identifying features to avoid detection by typical detection methods. Many common forms of malicious code can be polymorphic, including viruses, worms and trojans (Lord, 2020).
Rootkit	Malware which infects the operating system of a computerised device and uses stealth techniques to carry out a number of malicious processes. Rootkits affect both mobile devices and static desktop computers (Bickford et al., 2010).
Streaming	Content distributed via the internet which plays immediately without the necessity to download a file to a device.
Streaming Website	A website used to illegally access copyright protected content including, films, television, games, and other media.
Snapchat	A multi-media sharing social network where users enhance content with filters and effects to create video or photo stories for sharing with others.
Spyware	A type of malware which gathers personal information, steals sensitive data, or track online activity and sends the data to third parties, advertisers, or data analytic companies (Norton, 2020).
Tagging or Tagged	Identified by name and/or connected by active hyperlink to another social media profile.
Third Party App Stores.	Unofficial marketplaces where users purchase applications for Android devices.
Tor	A collective of volunteer operated servers which allow users to send data using a random pathway through several servers so that it is impossible to tell where the data came from or where it is going (TorProject, 2020).
Trojan	Malware disguised as legitimate software, typically controlled by third parties (Norton, 2020).
Twitter	Micro-blogging site to create short posts of content. Originally 140 characters long, Twitter now supports 280 characters per’ Tweet’.

Virtual Private Network	A secure, encrypted connection between a device and a server operated by the VPN service. Prevents interception of web traffic, hides an IP address, and aids safer internet use (Eddy, 2020).
Wiki	A website accepting contributions from any user, including making corrections, adding content, or editing.
Yantsi	A 'people-search' website which searches through multiple online platforms and returns content relating to individuals. For example, user accounts on social media, retail websites or articles in the online media.
Zero-Day Vulnerability	A vulnerability in computer software with no available 'fix' or 'patch'. The 'zero' represents the number of days that a patch has existed to repair the error in the code.
Zero-Day Exploit	Malicious code developed to take advantage of a particular zero-day vulnerability (Myers, 2015).
Zero-Day Malware	A term used by IT professionals to indicate a recently discovered strain of malware as a new threat. Zero-Day malware typically has limited defences (Techopedia, 2020).

Preface

DECLARATION

This work has not previously been accepted in substance for any degree and is not concurrently submitted in candidature for any degree.

STATEMENT 1

This thesis is being submitted in partial fulfilment of the requirements for the degree of Doctor of Philosophy (PhD).

STATEMENT 2

This thesis is the result of my own independent work/investigation, except where otherwise stated. Other sources are acknowledged by explicit references.

STATEMENT 3

I hereby give consent for my thesis, if accepted, to be available for photocopying and for inter-library loan, and for the title and summary to be made available to outside organisations.

Signed (candidate) Date ……02.07.2021

Abstract

This work presents a single methodology design across three different groups to chart the challenges and potential of digital investigation and to offer an original contribution to researchers seeking purposive samples specific to topical research questions. Open-source online intelligence theorised from an attacker's perspective is underpinned by a novel cyber-orientated framework of routine activity theory (RAT) (Cohen and Felson, 1979) to highlight digital footprint as a vector for targeted social engineering. Seventy-six (N=76) demographically diverse financial services employees from occupations throughout the sector provide empirical data via a mixed methods online survey. Cyber-specific RAT evaluates the 'average user' (with no specialist training) as a potential contributor to human assisted cybercrime threatening corporate networks through use of personal technologies and internet-based activities. Robust discussion debates routine digital activity using smartphones, tablets, and consumer Internet of Things (IoT) devices as an unmitigated factor for workplace risk. Personal internet use, devices accessing corporate networks, self-promotion on social media, physical and virtual IoT, executive personnel practicing 'unsafe' behaviours and assumed device security as licence for unrestricted online activity are key findings of this study which offers original contributions to critical assessment of insider threat. Despite employee (mis)use of personal technology as a potential vector financial organisations are seemingly unprepared for small-scale and dynamic risk. Results recommend bespoke training at all levels to associate personal use and online behaviour with known cyber risks and capacity for loss or harm. Cyber-RAT as a framework to identify suitable targets and potential for guardianship will contribute value added and assist in a more holistic response to cybercrime where the human element complements technological solutions as a positive enhancement to enterprise security.

Acknowledgements

Many thanks to Dr David Hicks who as Director of Studies was with me from the very beginning and fought my corner on several occasions. Without his calm support and sense of humour, this project would not have made it to the end.

Thanks also to Dr Phil Henry and Professor Philip Hodgson for all their assistance and input.

Thanks too, to all the unknown financial services employees who gave their time to volunteer, and Dave and Pip who managed without me for far longer than any of us ever expected.

Chapter One: Introduction

1.1 Introduction to Personal Technologies

The irrepressible progress of internet-connected services and the evolution of the networked society (Castells, 2005) have created a monumental transformation to the traditional model of society. Many previously physical amenities now favour a virtual residence on the World Wide Web and irrespective of personal competency, individuals are obliged to utilise networked systems. Access to utilities, services, entertainment and communication becomes limited without entering cyberspace. Mobile technology has replaced the static desktop computer as a gateway to the online environment (Clement, 2020b; Statista, 2019) and contemporary users prefer a web-enabled portable unit such as a smartphone or tablet. Smartphones and other mobile technologies have thus become indispensable, and many users own several devices to suit lifestyle or performance requirements. As a consequence, criminals devise increasingly sophisticated methods to exploit them, using numerous and variable threats shared via the internet.

Routine digital activity may expose an average user (without specialist skills or training) to an assailant, or a malicious instrument intended to harm. Personal internet activity may introduce malware to a device and risk can be exacerbated if no security mechanisms are enabled. A compromised phone or tablet brought to the workplace and given access to a corporate network may threaten digital infrastructure. If allowed to interact with other mobile units, an infected device might share harm through several communication methods. In the financial

industry, where networked systems deliver services and protect data, employee personal technology may introduce unexpected risk into an unprepared workspace. The sector acknowledges a continual threat of cybercrime and methods of resilience are undoubtedly employed by individual corporations. Nevertheless, year on year, cyber security services report that cybercrime instigated or abetted by elements of human behaviour continues to succeed (Symantec, 2019, Verizon, 2020). The average-user employee may be a contributory factor to workplace human-assisted cybercrime, and an unknowing or inadvertent consequence of using technology without comprehension or recognition of the risks.

Literature assessing employees and technology is plentiful, particularly in respect of systems or internet platforms used in the workplace (Byrne et al.,2016; Coles and Hodgkinson, 2008; Sjöberg and Fromm, 2001; Tsai et al., 2016). Nonetheless, modern workers may be carrying devices used first in personal space and later connected to a corporate network. Research discussing use of personal technology at work and home appears to be absent and other observations conclude that in place of employees, IT professionals are often the sample providing data regarding technology use at work (Györy et al., 2012; Kraemer, Carayon and Clem, 2009; OpenDNS, 2015; Silic and Back, 2014). To address these limitations and theorise whether personal technologies may exacerbate risk to a corporate network, it may be beneficial to examine routine digital activity conducted by employees who, physically and virtually, bring devices into the workplace.

The phrase ‘personal technologies’ is an umbrella term, to encompass any digital systems owned and used routinely by the average user and may include a smartphone, tablet or laptop. Digital activity can be defined as use of applications, entertainment and lifestyle platforms and other interactive internet services such as social media. Average-user activity in both personal space and the workplace should be examined and device access to the corporate network and presence of enabled security mechanisms confirmed or denied. A supplementary range of devices which fit into the category of personal technologies are consumer Internet of Things (IoT) devices or systems. ‘Smart’ technology is increasingly ubiquitous and personal IoT present in the workplace or accessed remotely by an employee may be an additional contributory factor to human-assisted cybercrime. As literature evaluating use of personal IoT as a risk factor does not appear to be available, evidence of workplace access, connection to the corporate network, or user-enabled security measures may be beneficial.

1.2 The Central Investigation and The Research Questions

This work aims to ‘bridge the gap’ between technology and the average user and will critically examine how use of personal devices may have unintended consequences to a corporate workplace. The research is not conducted from the perspective of an information technology professional and is instead implemented by a researcher outside the field of cyber security (see 4.3.2). This unique approach may thus identify whether average-user employees are unknowingly engaging in (in)appropriate cyber behaviour and introducing small-scale variable and dynamic risk to critical corporate systems. Results will challenge the traditional model of insider threat which currently designates the employee as

disgruntled, vengeful, incompetent or an extension to the reach of a physical attacker (Liang, Biros and Luse, 2016; Mouton et al., 2014; Saxena et al., 2020; Warkentin and Willison, 2009). Accordingly, the research questions are based in methodology and grounded in interpretivist epistemology to seek empirical evidence of employee behaviours. The three questions are presented as follows:

- What are the actual rather than the perceived risks created by personnel within a financial organisation? (**Research Question RQ1, actual/perceived risks**)
- How does an average user utilise their own mobile device(s), and how may this impact on the corporate IT infrastructure? (**Research Question RQ2, average usage/impact**)
- Are devices and applications associated with the Internet of Things establishing a presence in the workplace and what unexplored risk might this entail? (**Research Question RQ3, IoT unexplored risk**)

The research objective is to encourage financial corporations to reconsider the employee as an insider threat on account of contemporary culture and a society dependent on technological lifestyle. An ideally suited purposive sample of financial employees who regularly undertake digital activity will be recruited to provide empirical data by completing a mixed methods (Bryman, 2012) electronic research instrument. Research methods will consist of open-source digital investigation utilising publicly accessible user-generated content combined with online resources to identify the sample. The three methodology chapters should be considered as one single methodology divided into separate parts to emphasise the different approaches taken during the digital investigation. The

individual chapters form a coherent whole and are indicative of the challenges of online research, thus, Chapters Four, Five and Six will chronologically document the journey towards data collection. Each chapter will demonstrate the flexibility and tenacity required for digital investigation and the final sample of seventy-six (N=76) financial sector employees should validate the choice of methods.

1.3 Theoretical Frameworks

A crime prevention framework suited to theorising risk occurring from regular use of technology is Routine Activity Theory (Cohen and Felson, 1979). When augmented with elements of Liquid Modernity (Bauman, 2000) to validate the fluidity enabled by cyberspace, routine activity theory (RAT) may be transposed to the digital domain as a cyber-specific theoretical model. The novel cyber-RAT framework will underpin the methodologies in conjunction with a social engineering template (Mouton, Leenan and Venter, 2016) to guide the digital investigation wherein the researcher will be mimicking an attacker seeking a candidate for targeted attack. Cyber-RAT will identify the internet user as suitable target whilst user-generated content which might be exploited during social engineering will confirm suitability as a participant. Respondent data will be critically analysed using the cyber-specific routine activity framework to theorise the employee or organisation (or both) as suitable target. In the discussion (Chapter Nine) the framework will offer opportunity for capable guardianship to assist with small scale risk mitigation.

1.4 Original Contribution

The research presented here offers a variety of original contributions. Although three methodology chapters is unconventional, they are indicative of challenges

and possibilities of digital investigation and are roadmaps that may be replicated and elaborated by other researchers. The methodologies demonstrate a practical application of the cyber-specific RAT framework, and offer novel contribution to technological risk assessment, with value for training, awareness, or policy development. Findings address the gaps in the literature; all data is provided by employees, focuses specifically on personal technology and evaluates consumer IoT as a risk factor. Results show that routine digital activity, personal technologies accessing corporate networks, physical and virtual presence of consumer IoT, senior personnel as practitioners of 'unsafe' behaviours and assumed device security as licence for unrestricted online activity augment the currently perceived model of insider threat. A major contribution is evidence that despite employee (mis)use of personal technology as a contributor to insider threat, financial organisations are seemingly unprepared for such small-scale and dynamic risk. The sector may aim for resilience against external actors and advanced cyber-threats but are reluctant or resistant to acknowledge the employee and their use of personal devices as a potential cyber-risk factor.

1.5 Thesis Arrangement

The work is arranged as follows: Chapter Two borrows suitable target, motivated offender and absent capable guardian from routine activity theory (Cohen and Felson,1979) and redefines cyberspace using liquid modernity (Bauman, 2000) and fluidity of contemporary, 'tech-driven' society. Elements of traditional routine activity theory (RAT) suggest habitual average-user *digital* activity may establish the suitable target. Cyber-specific RAT frames the research questions and actual and theorised risk in the context of potential convergence with a human criminal

or digital instrument intended to extend the reach of an offender (see 2.3.1). The impact of active and passive data as digital footprints (Fehér, 2017) determines the basis for open-source research, to be introduced later as the research methods beginning in Chapter Four. The remainder of Chapter Two transposes rudiments of traditional RAT to the cyber domain to validate the theoretical Cyber-RAT framework, introducing internet threats, malware and other technological issues to emphasise target and offender in physical and virtual space. The chapter concludes with a visual representation of cyber-RAT (Table 2) as an aid to evaluate the remainder of the thesis.

The literature review in Chapter Three outlines the financial sector response to the threat of cybercrime (BoE, 2020) and suggests limitations in the bespoke threat assessment process (3.2). Reliance on technological solutions may be vital to safeguard IT infrastructure but dependence on software and digital systems may be unable to prevent incidents if the (un)witting instigators sit inside a corporate firewall. To consolidate the necessity for a revision of insider threat to reflect contemporary lifestyle, 3.2.1 will consider the literature to emphasise deficiencies in the current model of deliberate or accidental harm (Liang, Biros and Luse, 2016; Mouton et al., 2014; Saxena et al., 2020; Warkentin and Willison, 2009). The technological risks briefly introduced in Chapter Two are explored in detail from 3.3 to 3.8 as a prelude to theorised augmentation of the ‘insider’ using synthesis of the threat landscape in the context of the post-millennial employee. The chapter concludes after introducing the smart technologies intended to enhance the health and living experience of the consumer (3.11) combined with the security risks observed by professionals in the security industry.

The methodology documented in Chapter Four, ‘The Corporate World’, begins by positioning the researcher in constructivist ontology to justify an interpretivist epistemological approach to a digital investigation underpinned by the frameworks of cyber-RAT and social engineering (Mouton, Leenan and Venter, 2016). The chapter outlines ethical decision-making during online research and records the preparations for safeguarding. The methods to conduct exploratory research to recruit a purposive sample of financial sector employees are presented chronologically to emphasise the necessity for creative thinking and tenacity during digital investigation. Chapter Five, ‘Executive Risk’ records a change of direction in research methods whilst remaining grounded in determination to obtain an ideally suited sample drawn from financial sector organisations. The chapter presents a synthesis of thirteen sequential investigations evaluated using the two theoretical frameworks to conclude suitable target and organisation at risk of convergence. ‘Executive Risk’ records a successful outcome resulting from knowledge sharing with financial corporations later usurped by suspected “question threat” (Foddy, 2011, p.117) and an assumed fear of reputational damage (Kember, 2018). Chapter Six, ‘A New Direction’ is presented in two segments, ‘New Methods’ and ‘Final Methods’. The final methodology remains true to the premise of purposive financial sector sampling but gradually deviates from an open-source investigation to a desperate quest for primary data, finally resolving successfully when completed surveys were received. Chapter Six closes with a review of the research instrument in respect of observed limitations and data cleansing ready for analysis.

Chapter Seven begins by presenting quantitative data extracted from the results to establish the seventy-six respondents (N=76) as average users of digital technologies as per the requirements of the central investigation. The remainder of the chapter presents empirical evidence applicable to **RQ1 actual/perceived risk** and **RQ2 average usage/impact** in conjunction with critical analysis supported by the cyber-RAT framework. The analysis focuses specifically on the user as a suitable target instigated by potentially 'unsafe' digital activities. These include (amongst others) streaming media content, gaming, adult entertainment and social media where encountering malware or other harm is a possibility (Fact, 2017; Grustniy, 2018; McGuire, 2019; Perekalin, 2019; Sood and Enbody, 2011). Chapter Eight continues with the response to the research questions and expands to include the IoT survey and **RQ3 (IoT unexplored risk)**. The chapter records qualitative data drawn from comments left by respondents to enhance and validate their electronic responses. Cyber-RAT and themes detected in the literature drive the critical evaluation of respondent behaviours and conclude with evidence of potential for small scale dynamic and variable risk.

Chapter Nine synthesises key findings from the results to corroborate risk observed during the digital investigation recorded in Chapters Four and Five and evidenced in the critical evaluation of respondent data. Robust discussion drawing on the literature helps to demonstrate the value-added offered in 1.4. The debate elaborates on novel observation to affirm personal technology use and 'unsafe' behaviour as a potential risk factor to a corporate workplace and identifies that senior executive are the personnel likely to indulge in 'unsafe' practices. As a solution, cyber-RAT is proposed as an enhancement to risk

awareness or to aid bespoke cyber training. Instead of a generic “fear appeal” (Johnston, Warkentin and Siponen, 2015, p.114), a user’s personal digital activity can be evaluated for suitable target and opportunities for capable guardianship.

In Chapter Ten, the thesis concludes that human-assisted cybercrime may be an (in)advertent consequence of using personal technology without comprehension of risk. Users who believe that guardianship is present may be unwittingly risking devices whilst undertaking unrestricted digital activity. Those who choose to bypass basic security may be knowingly leaving a device vulnerable to harm but are inadvertently uninformed of the risks enabled by their unique internet behaviour. Personal reflection is offered to evaluate the research instrument and the limitations of interpretivist ethical decision-making. To address the inadequacies of this study, recommendations are made for further academic research. All charts and tables used to illustrate the written work have been generated by the author, unless otherwise indicated by citations.

1.6 Additional Resources for the Reader

This thesis will encompass human behaviour, risk awareness and criminology, and will focus on the social, rather than the technological aspect of cybercrime. Incident or crisis management and protection of corporate networks will not be attempted, nor will effort be made to explain why or how individuals commit cybercrime. Despite in-depth analysis of internet user behaviour, the narrative will not comment on identity assumed by individuals when interacting with online audiences. The topic of precedence is average-user digital activity in the context of potential risk to oneself and others, and a users’ persona and desire to be

‘liked’ is not relevant here. Readers interested in the topic of online identity in personal or professional practice may find other authors of value, including Davis (2014); Jawed, Mahboob and Yasmeen (2019); Jordan (2019); Kim, Lee and Oh (2020); and Poletti and Rak (2013).

Security experts assert that cybercrime may be reduced if users were aware of risks to an organisation and encouraged to make concerted efforts to avoid them (NCSC, 2018a). Despite the benefit of raising user awareness, Information Technology (IT) specialists and technicians tend to communicate using a befuddling language of jargon and complex terminology. The media likewise confuse the average user with talk of zombies, botnets, trojans and worms. Accordingly, only those with specialist training or specific interest are likely to be passionate about computing matters. Nonetheless, to comprehend the rationale for this research it will be necessary to discuss pertinent elements of technology. Throughout the narrative, any necessary technical explanation will attempt to refrain from losing the interest of generalist readers via overuse of unclear vocabulary and terminology. The glossary may assist with unfamiliar terms and readers will be directed to additional information accordingly. For those interested in learning more about cyber security and internet threats, work by Ivančík (2020); Jeske and van Schaik (2017) and Ramakrishnan and Tandon (2018) may be useful resources.

Chapter Two: The Theoretical Framework for RAT in Cyberspace

2.1 Introduction

This thesis does not intend to debate the (relative) value of RAT when applied to the digital domain but instead suggests that theoretical transposition of essential RAT fundamentals to cyberspace may stimulate discussion and new perspectives when assessing workplace technological risk. The central investigation may be seen as grounded in cyber-specific routine activity theory: **RQ1 actual/perceived risk** evaluates digital activity as a vector for convergence with an offender, **RQ2 average usage/impact** queries personal technology use as instigator of suitable target and **RQ3 IoT unexplored risks** debates emerging technologies in the context of absent guardianship. The following discussion of routine activity theory and overlap with the digital domain will propose a theoretical model to frame the study and establish a basis for the unconventional methodologies presented later in Chapters Four, Five and Six. Chapter Two is structured as follows: Section 2.2 reviews the traditional 'real world' crime prevention framework of Routine Activity Theory (Cohen and Felson, 1979) to establish suitable target, motivated offender and capable guardian. Section 2.3 frames average usage of personal technologies as routine digital activity. Section 2.4 shifts the traditional model to the cyber-domain, suggesting how time and space may be represented virtually and 2.5 demonstrates the cyber-equivalent of fundamental RAT elements including observed guardianship and target attractiveness. Section 2.6 suggests the average user of technology as user-guardian and 2.7 offers a practical application of cyber-RAT establishing fluidity between target, offender and guardian. The close of the chapter offers a visual representation of the theoretical

framework (Table 2, 2.7.4) to aid evaluation of the literature review in Chapter Three, the methodology chapters and assist with critical analysis and evaluation in response to the research questions (Chapters Seven, Eight and Nine).

2.2 A Brief Introduction to Routine Activity Theory

Routine Activity Theory is a framework allegedly amongst the "most influential theoretical constructs" cited by criminologists and academics specialising in crime science (Miró, 2014, p. 1). To successfully prevent crime, an understanding of the nature of the criminal activity is required, alongside preventative methods to address the problem. This is then augmented by persuading people and organisations of the value of implementing potential solutions (Sampson, Eck and Dunham, 2009). Accordingly, the RAT framework is recognised as a method of understanding the circumstances which allow criminal activity to occur. RAT suggests that opportunity for crime arises when three significant conditions are met. Specifically, the "convergence in space and time" of a suitable target, a motivated offender, and "the absence of capable guardians against a violation" (Cohen and Felson, 1979, p. 589). The exposure of a likely target to a potential offender is determined by habitual activities, and the daily routines of both individuals and demographics are associated with criminal victimization (Tewksbury and Mustaine, 2003). The three necessary RAT conditions can be defined as: "someone liable to commit a crime", "a person or thing that the offender will focus on" and the absence of "someone who is able to protect the target" (Tilley, 2009, p. 120).

Traditional RAT defines routine activity as “recurrent and prevalent” actions which satisfy individual or populational needs occurring sufficiently to “make them part of everyday life” (Cohen and Felson, 1979, p.593). Taking place in the home, at work or other locations, activities may include employment, food provision, social interaction and leisure. Expanding on the proposal that lifestyle of demographics may be an element in victimisation (Tewksbury and Mustaine, 2003), activity taking place on a semi-regular basis may also be construed as routine. An example of this might be young people attending music festivals throughout the summer season.

In the original theory (Cohen and Felson, 1979), the motivated offender is introduced as “a rational criminal who takes advantage of opportunities” (Miró, 2014, p.5) to conduct “direct contact predatory violations”. Physical interaction takes place between “at least one offender and at least one person or object” (Cohen and Felson, 1979, p. 589). An offender may “violate rules” and is thought to be the “immediate cause of a crime” (Sampson, Eck and Dunham, 2009, p. 39). The suitable target is identified to an offender through routine activity, with suitability judged on “real or symbolic” value and a consideration of physical obstacles, visibility and access (Miró, 2014, p. 2). A target may be a physical person, property or other goods, and routine activity will also have impact on location and whether the target is in a visible or accessible place at any particular time (Cohen and Felson, 1979, p. 591). Those who visit bars and drink alcohol in the evening allegedly have higher rates of victimisation. Additionally, males, as they spend more time outside the home environment (Pizarro, Corsaro and Yu, 2007, p. 377).

For criminal victimisation to occur, offender and target must converge in space and time in the absence of a capable guardian. Guardians in traditional RAT are varied and can be found in different contexts including dogs, cameras and other tools which "reinforce guardianship" (Hollis, Felson and Welsh, 2013, p. 67). Guardians are typically "ordinary citizens" going about their business, subsequently providing guardianship "of one another and of property" (Cohen and Felson, 1979, p. 590). Guardians can also be individuals specifically employed to offer protection or may be large groups of strangers who by sheer volume of numbers create protection (Sampson, Eck and Dunham, 2009). As an example, guardians against a burglary may be occupants in residence, an alarm system, a dog in the role of occupancy proxy, property location and visibility to neighbours (Roth and Roberts, 2015, p. 121). Other literature discussing RAT expands on the original model to create sub-categories of guardianship in the form of handlers, managers, controllers, and super-controllers. These classifications thus increase protective qualities (Sampson, Eck and Dunham, 2009).

RAT has been successfully applied to burglary (Roth and Roberts, 2015) and homicide (Pizarro, Corsaro and Yu, 2007). Traditional theory has also been used to identify patterns in online behaviour which then influence theft in the physical world (Lee et al., 2018). Nonetheless, the success of RAT when used as an explanation for occurrence of cybercrime is often a subject for debate. Some scholars agree it has a purpose (Grabosky, 2001), and others dissent (Yar, 2005). The next section (2.3) will begin the discussion leading to a proposal for a novel association between traditional RAT and present-day cyberspace; beginning with the internet and the data trail created by routine internet activity.

2.3 The Internet for All

The technological topics introduced in this section are briefly alluded to, rather than elaborated upon at length. Detailed explanation will be found in the literature review (Chapter Three, commencing at 3.3).

In recent years, a decline in physical customers has affected the business model of retail outlets, banks, and estate agents (Hardy, 2018; The Telegraph, 2012; Treaner and Collinson, 2017; Wearn, 2016). Numerous enterprises have reduced or ceased a 'real world' presence and moved to a virtual existence. Many public services can only be accessed via the internet (Asthana and McVeigh, 2010) and physical offices offer limited support, with service-users signposted to websites and online assistance instead. The shift to digital provision occurred as electronic delivery is efficient and cost effective and customers (appear to) favour access provided by internet facilities, in particular mobile technologies and banking applications (apps) (Jones, 2016). The switch to online services has necessitated a requirement to access the internet or face exclusion from the benefits and entitlements facilitated by digital inclusion (West, 2018). The online migration coincided with a proliferation of messaging and communication technologies which allow networked relationships to flourish, regardless of geographical location. These services have prompted older people to engage more with the internet, shop online (ONS, 2019) and embrace social media (Ofcom, 2017), and all demographics use internet communication services and applications (Sweney, 2019) accessed via smartphones and tablets (Ofcom, 2018). Routine internet use and online services have become firmly established in contemporary culture.

The outcome of more demographics habitually using the internet is increased potential for any user, irrespective of race, wealth, status, age, or intelligence to become a victim of cybercrime. The media relishes sensationalist coverage of cyber-attacks (BBC News, 2018; Bond, 2018; Graham, 2017; ZDNet, 2018) and average users may believe that only corporations or individuals with great wealth are targets. Nonetheless, all internet users may be at risk, not only from targeted crime, but from random attacks and victimisation by circumstance (Thornton-Trump, 2018). The 2019 Crime Survey for England and Wales (CSEW) estimated that nine hundred thousand (900,000) computer misuse crimes affected the adult population (Stripe, 2020), including viruses, hacking and fraud (BBC Bitesize, 2020). Henceforth, this study will adopt the philosophy of Cohen and Felson (1979, p. 589), to "take criminal inclination as given" and surmise that *any* routine internet activity has the potential to facilitate convergence with a motivated offender.

The focus of the study is the average user with no specialist skills or training who regularly utilises personal technologies. Although those who recognise internet risk may employ advanced methods of online protection, for example, a virtual personal network (VPN) or firewall device (see Glossary), this research seeks mobile device users who may or may not protect routine activity with basic security in the form of antivirus solutions and regular updates. For these users, the assumption that *any* internet activity involves an element of risk may be valid, as Chapter Three details a succession of threats and harms to which all who access cyberspace may be vulnerable. For the reader interested in exploring

additional options to enable safe internet activity, please see Poremba (2018); Rouse and Burke (2020) or Stanojevic (2020).

2.3.1 Routine Cyber Activity

With so many facilities available, daily internet activity may involve multiple services, including banking, shopping, paying bills and accessing public resources. Users can conduct business administration or remote office working. Leisure time may be spent streaming media content, playing multi-user games, or interacting with others via telecommunications software such as Skype, or Zoom. Social media and communication applications such as WhatsApp may be used throughout the day for dialogue with colleagues or to update family or friends. Even “narrow” internet users (Ofcom, 2019, p. 20) so-named due to minimal engagement and limited range of internet activity, will routinely access email (Ofcom, 2018, p.192).

Although the internet has changed lives and working practices, “technological advances designed for legitimate purposes ... may enable offenders to carry out their own work more effectively” (Cohen and Felson, 1979, p. 591). In parallel with routine ‘real world’ activity, regular internet access and online practices may expose a user to a motivated criminal or ‘instrument’ used to instigate victimisation. To place the concept of ‘instrument’ in context, hyperlinks infected with malware placed on social media sites, or fake or compromised websites may all extend the reach of an attacker. Furthermore, whilst traversing the facilities of the online environment, a trail of data is left by the user. These ‘digital footprints’ (Fehér, 2017, p. 112) may be exploited by a threat actor and place even a casual

user in a position of victimisation. In the context of **RQ1 actual/perceived risks** this routine digital activity and the associated data trail may subsequently introduce harm to a financial workplace.

2.3.2 Digital Footprints: Passive Footprints

For many demographics, the internet has usurped encyclopaedias and directories as a resource for seeking information. A digital native who has always used technology and is a "native speaker of the digital language of computers" (Prensky, 2001, p. 3) is unlikely to use paper resources when Wikipedia or Google are available. Prior to digital resources, a personal quest for knowledge would be private, with no easily accessible traces to indicate to others what a seeker was looking for. In contrast, an online search for information or products leaves a history of what is sought, and any places visited on the internet whilst seeking. The inadvertent trail of data compiled during online activity is named a "passive digital footprint" (Techterms, 2014) and a user adds to it unknowingly and sometimes without realising that data is being collected. Micheli, Lutz and Büchi (2018) propose two types of passive footprints. Those generated as an outcome of a user's interaction with an internet platform and others created from data posted by other users which is "linked to an individual" (Micheli, Lutz and Büchi, 2018, p. 6). Footprints resulting from user interaction include the internet protocol (IP) address (see Glossary), visited websites stored as search history, and geolocation services used to accurately establish locale (Norton, 2019). Passive content produced by other users includes "tagging" (Micheli, Lutz and Büchi, 2018, p. 6), when social profiles or names are attached to online content, images and "endorsements, ratings, and comments" (Micheli, Lutz and Büchi, 2018, p. 6).

Research has found that passive data from routine internet activity can be retrieved from a computer system even if a user has activated controls to enable private browsing (Ohana and Shashidhar, 2013, p. 10). Cached images, URL (the address of a web page) history and usernames with accounts may be accessed during forensic investigation. The footprint generated by others, described by Micheli, Lutz and Büchi (2018) is typical of social media activity, but users outside an immediate network may additionally contribute to passive content. For example, organisers of business events such as conferences may name delegates. Charity events and private fundraising is frequently reported online. Community or church newsletters are published to local websites and a social media profile for a town or village may report on civic happenings and list participants at meetings or public occasions. Corporations may publish information about an employee on a company website or post images of events or awards ceremonies on social media pages. In the context of **RQ1 actual/perceived risks,** passive data concerning employees may constitute risk of targeted social engineering (see 3.4.1). Employees using personal devices may also succumb to phishing attacks (3.4.2) enabled by passive data and are relevant to **RQ2 average usage/impact.** Open-source intelligence (OSINT) (see 2.3.7) can obtain passive data by dynamic keyword searching utilising the Google search engine and will be demonstrated in the methodology chapters commencing at 4.6.

2.3.3 Digital Footprints: Active Footprints

Active digital footprints are created as a result of overt online behaviour and comprise any internet activity intended to be seen or shared by others

(Techterms, 2014). Social media content is a good example, and may include "self-authored" text, images, and video (Madden et al., 2007, para. 1). Users frequently share "immediate thoughts, emotions and beliefs" and personal data, for example "age, gender orientation, place of residence" (Azucar, Marengo and Settanni, 2018, p. 150). Maintaining a 'wish list' of coveted items via an account on an online retail platform or posting a review of recent purchases will additionally add to a footprint. Likewise, partaking in social curation, for example using Pinterest to collect, categorise and share digital objects, and to comment and 'like' the collections of others (Hall and Zarro, 2012). Users playing games with other gamers via online platforms often share content via social media. Consoles such as Play Station and Xbox connect to the internet and share "hi-scores, game achievements and recorded videos" (Davies et al., 2015, p. 82). The online media may post coverage of an event where the individual was a speaker or organiser, or the user may have been an interviewee. Once a name appears in an online newspaper report, the media content adds to the footprint. Other forms of active data include user-published content to blogs or wikis (see Glossary), user-comments in response to other peoples' content seen on websites, blogs, or social media profiles and "liking, favouriting, following" (Micheli, Lutz and Büchi, 2018, p. 6). Table 1 (below) illustrates active and passive digital footprints.

Fehér (2017, p. 112) suggests that behind each footprint is a "decision chain" where the user has made a "choice relating to the control of public and/or private data and the (self) consciousness/awareness of digital activities". This may be summarised as a conscious decision to make selected data public, for example,

Active Footprints : Generated as an outcome of intentional online behaviour	Passive Footprints: Generated unintentionally during internet use, sometimes without users' knowledge
Includes content published to social media sites, websites, blogs or wikis	Includes data collected by websites including IP address, type of device and location
Images of, or taken by, the user with tags to names or social media profiles	Websites visited online can be stored as web browser history
Comments responding to published content, reviews and endorsements	Includes comments made by others on social networks, tagging images or linking content to an indivual or profile
Responses made by the user to online content, using a username, real name or linked to social media profiles	May also include other inernet activity the user does not know about e.g. Media articles, company reports published online, community newsletters, sports results.
Curated content on image sharing sites	
Scores, achievements, videos shared by online gamers	
Sports accomplishments , fundraising pages	

Table 1. Active and Passive Digital Footprints

social media content relating to a business enterprise; and to retain control over data intended to be private, such as family life. Users may have awareness that passive content can be generated as a result of digital activities but in the previous example, passive data may assist with business promotion and increase customer footfall and is therefore encouraged. Nonetheless, generation of passive content beyond the comprehension of the user may undermine the conscious decision model. An example from 2018 is the visualization map generated by user-data uploaded to Strava, a social network for athletes. The Strava application recorded users' fitness achievements and shared them with others, but additionally aggregated all the user-data into a global interactive map (Hern, 2018a). The map made it possible to recognise popular running routes and analysts realised that US military bases, a Special Air Service base and

GCHQ (Government Communications Headquarters) in the UK were visible (Field and Murphy, 2018). In this example, military personnel on active service had used Strava to record their fitness and used the facilities of the app to consciously add to active footprints. The passive data which displayed the location of secure military and government operations was beyond the comprehension of the user and undermined the effectiveness of the decision chain.

A user does control the decision to enable personal privacy controls, and this may additionally represent the self-consciousness or awareness as indicated by Fehér (2017, p. 112). The Strava fitness app has privacy controls to make the users content private and disable the mapping feature (Field and Murphy, 2018). The users whose data contributed to the interactive map may have self-consciously elected to forgo security options, with the intention of making data public. If the military personnel had understood the eventual consequences, the decision may have been different. The Strava example indicates a lack of user awareness about how personal use of technologies may have impact and is a topical reference to the relevance of this research study.

2.3.4 User Augmentation

Many average users interact with friends and followers on social networks and anticipate generating "highly visible metrics of popularity and endorsement" (Khamis, Ang and Welling, 2017 p. 196) in the form of 'likes', positive comments or visual responses. For many users, footprints augmented by other users "may produce both desirable and profitable consequences" (Micheli, Lutz and Büchi, 2018, p. 6). In the context of **RQ1 actual/perceived risks,** a 'tagged' image

where a user is identified by name and/or connected by active hyperlink to another social media profile (Facebook, 2018) may be another example of passive content with no user awareness. As an example, to place this in perspective, a photograph taken at a family event may be posted to a social media profile. Friends and followers can share the image and add tags, thus identifying people in the photograph and creating links to profile pages. If an individual is not a regular social network user or has disabled the notifications sent from a social platform to notify them that a tag has been made, the individual may be unaware they have been identified on social media (Ramsey, 2019).

To prevent passive social media data from becoming publicly accessible, and to retain control overactive footprints, a user has the option to activate privacy mechanisms and place restrictions on who may view personal data. The social site Instagram may have less than twenty-five percent of accounts protected by privacy since the default setting is for accounts to be public (Das and White, 2019). Thus, ideally, Instagram privacy options should be explored, and a level of privacy enabled to suit individual users, a further example of Fehér's (2017) decision chain. Diligent control of privacy requires similar motivation from all participants in a social group as one unprotected profile may provide access to data shared between the network. Regardless of efforts to safeguard data, a user who self-consciously or unwittingly neglects privacy compels a group to abide by their decision. Hicks (2018b) suggests this may be termed "the lowest common denominator decision-chain model". In the context of the central investigation active data unprotected by privacy controls may be a potential contributor to risk of social engineering (see 3.4.1) and relevant to **RQ1 actual/perceived risks**.

Since ninety-nine percent of social media users utilise mobile devices for social networking (Statista, 2020b) unprotected data produced by personal device use has relevance to **RQ2 average usage/impact**. The methodology chapters will demonstrate unprotected data in the context of suitable target, commencing in Chapter Four at 4.6.

2.3.5 Impact of Digital Footprints

Young people in particular are advised to exercise caution, not only with privacy but with what they share to their network; as Conlin (2006, cited in Fehér, 2017, p. 113) accurately states, "you are what you post". Inappropriate or malicious content may attract the attention of law enforcement or be copied and shared, thus removing it from the control of the user who can no longer delete it, even if they choose to do so (Childline, 2018). Colleges and universities may conduct online searches to investigate prospective students and an active footprint displaying dubious activity, for example, substance abuse or immoral behaviour may affect a young persons' chance of study at a chosen venue (ibid., 2018). Recruiters often inspect social media content to assess suitability when a candidate applies for a position in their company (Smejkal, 2017) and public content may affect a candidate's prospects. Furthermore, any content that a user 'likes', 'shares' or 'follows' gives the impression of endorsement. This may subsequently affect professional credibility or mar the reputation of their employer (Juba and Young, 2018).

2.3.6 Erasing Data

An active footprint will remain indefinitely on the internet unless a user is proactive about managing retrievable data. Appendix A briefly summarises the General

Data Protection Regulation (GDPR) and 'the Right to be Forgotten' (ICO, 2020a) in the context of erasing digital footprints. Readers wishing to know more about data protection legislation and the GDPR may find the Information Commissioners Office Guide to Data Protection of interest. An online resource available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/.

2.3.7 Active and Passive Data as Intelligence Tools

Table 1 in 2.3.3 illustrated sources of passive and active data as 'footprints' available on the internet. Digital investigation using open-source intelligence (OSINT) utilises 'footprints' found in publicly accessible internet resources including (amongst others) government databases, libraries, archived newspapers, magazines and corporate and third sector publications. Tools to assist searching through online content to retrieve footprints include search engines, for example Google which may be modified for custom searching within specific parameters (see 4.6 for a comprehensive discussion of OSINT tools and techniques). Information gleaned from social networks may additionally be utilised for investigatory purposes. Intelligence extracted from "social media content authorised for public access" (Omand, Bartlett and Miller, 2012, p. 805) is known as SOCMINT, drawn from SOCial Media INTelligence (Galloni, 2018). Law enforcement officers may be trained to use SOCMINT to aid criminal investigation (Smith, 2013; Smith, 2014). Content can be a valuable resource to "identify networks and movement through social 'shares' and interactions" (Galloni, 2018, para. 10). Furthermore, asset tracking and recovery is assisted through content analysis (ibid., 2018, para. 8) and insurance, benefits and trading

standards investigators use SOCMINT to search for evidence before processing claims (Smith, 2013; Smith, 2014). Two of the methodologies (Chapter Four, 'The Corporate World', and Chapter Five, 'Executive Risk') will demonstrate how SOCMINT might be used as a resource by offenders when formulating an attack through social engineering.

2.4 Routine Activity Theory in the Cyber Domain

There have been previous academic attempts to associate theories explaining 'real world' crime with offences committed on the internet (Leukfeldt and Yar, 2016, p. 263). In the physical world, RAT requires a convergence of offender and target, and the absence of a capable guardian. Thus, arguments against applying the framework to the cyber domain imply that the construct of cyberspace cannot satisfactorily meet the requirements of traditional RAT. Cyberspace is "manifested in anonymity in space and time, immediacy of effects, non-attribution of action, and the absence of any international borders" (Mittal and Sharma, 2017, p. 1347). To expand on the lack of borders, an offender and target are very unlikely to be in the same location, for cyberspace permits interaction between users who may be on different continents. Hence, "without the ability to identify relations of proximity or distance between offenders and targets" (Leukfeldt and Yar, 2016, p. 265), the argument exists that cyberspace cannot provide the element of space and time so crucial to RAT.

2.4.1 Time and Space in the Virtual World

Despite any academic debate, it may be argued that time and space still exist for both the target and offender (Hicks, 2018b), although not the conventional

existence presented by the physical world. The parties do not need to access the internet at the same time, nor be in the same locality. To place this scenario into a practical context, consider a user who routinely accesses social media in the evening. The physical offender may not be online at all, but an instrument to extend the offenders' reach is present, in this example as a malicious hyperlink on a social media profile leading to a sensationalist piece of celebrity gossip. The length of time spent online is irrelevant, the user's *presence* in cyberspace is sufficient to attribute status as suitable target. Thus, the crucial 'space' is the hazardous Facebook profile, and the 'time' is the moment the user accesses (clicks on) the malicious hyperlink. Without a capable guardian in the form of user awareness to avoid the hyperlink, or robust antivirus to prevent the malware from invading the targets' device, victimisation may occur. This virtual scenario has relevance to both **RQ1 actual/perceived risks** and **RQ2 average usage/impact**.

Capable guardianship in the context of traditional RAT is "a critical determinant of victimization" (Reynald, 2010, p. 359) and a cyber-specific perspective additionally suggests that guardianship is key in the digital domain. Tilley (2009, p. 120) suggests that credibility of guardianship may have greater value than capability and uses an example of closed-circuit television (CCTV) as a deterrent to crime incidents, despite the poor functionality of the devices in question. In the physical world, credibility may indeed be a factor to successful prevention of victimisation and a contemporary example substitutes CCTV for internet-connected surveillance cameras. Such devices in a visible location may have credible guardianship qualities regardless of whether they function or are even connected to an electricity supply. Nonetheless, in the cyber domain, it may be argued that a

robust and capable guardian may be more efficient than a credible one. As an example, antivirus software downloaded for free from an acknowledged supplier may give the impression of credibility but if the functionality of the software is incapable of preventing internet harms then it lacks intrinsic value as a guardian. It may be preferable to purchase robust antivirus solutions with the capability of offering actual protection.

Literature denying the similarity between physical and cyber-RAT dissects cyberspace in a detailed and logical manner (Leukfeldt and Yar, 2016; Yar, 2005) and a myriad of differences cannot fail to be observed. RAT is thus rejected by some as an acceptable theory when applied to an online context. Nonetheless, this work will propose that elements of RAT might successfully transpose to the digital arena. Section 2.5 will begin to equate the fundamental components of traditional RAT to their virtual counterparts to create a theoretical cyber-RAT framework. Section 2.6 suggests the average-user as capable guardian and 2.7 provides examples to determine how cyber-RAT might be applied to end-user internet crime scenarios, validating the concept of 'fluidity' in cyberspace, with elements drawn from liquid modernity (Bauman, 2000) (2.7.2). The final part of this chapter provides an illustration of the cyber-RAT framework (Table 2, 2.7.4) deliberately placed in the concluding section to visually contextualise the discussion of RAT in cyberspace and reinforce the rationale prompting the novel theoretical modelling.

2.5 Cyberspace is Different!

Literature often compares the online environment with the 'Wild West' (Hymas, 2020; Kounalakis, 2018; Look, 1999) to illustrate a place where normative values do not apply and there are no controls, other than an unwritten 'netiquette' (Hodges, 2002) (see Glossary). Cyberspace has been described as a socio-technically generated interactional environment (Castells, 2002, cited in Yar, 2005) "discontinuous with the terrestrial world" (Leukfeldt and Yar, 2016, p. 264) and transnational and de-centralised (Capeller, 2001, p. 233). The internet has the "capability to throw surprises with rapidity" (Mittal and Sharma, 2017, p. 1343) and contains content both "fleeting and volatile" (Capeller, 2001, p. 233). Ultimately, the lack of official supervision over behaviour of users has facilitated the opportunity for criminal victimisation (Maimon et al., 2013). To accept that rudiments of traditional RAT may apply to cyberspace, it must be appreciated that cyberspace is fundamentally different with a "unique characteristic" (Mittal and Sharma, 2017, p. 1343). Without this acceptance, zealous analysis will always find ways to contradict the theory. This researcher argues that the concept of motivated offender, suitable target and absent guardian can apply, even if the application may seem 'discontinuous' to traditional theorists.

2.5.1 Physical RAT and Cyber-RAT – not so different after all?

In their paper introducing routine activity theory, Cohen and Felson (1979) referred to offenders as 'motivated'. Later literature by the authors avoided the reference, for the relevance for RAT was not a motivation to commit crime, instead that "physical factors made it possible for a person to be involved in crime" (Miró, 2014, p. 2). When applying the RAT model to the cyber domain, the

motivation of the offender is not always the pursuit of a particular victim, rather that the virtual presence of the user in cyberspace places them in the position of suitable target (Thornton-Trump, 2018). Thus, the physical factors of offender and target accessing cyberspace without the presence of a capable and active guardian can allow victimisation to take place.

Physical world offenders typically prefer to conduct criminal activity in areas they know well (Brantingham and Brantingham, 1991) or carry out long-term activity in familiar cities or neighbourhoods where they may have well-established social relationships with co-offenders (Leukfeldt, Kleemans, and Stol, 2017). In comparison, criminals with the knowledge and capability to abuse digital technologies are also operating in a familiar and well-known area. Their neighbourhood is cyberspace, and online resources such as fora may enable social relationships between international co-offenders (Leukfeldt, Kleemans, and Stol, 2017). Instead of cyberspace existing as a vast, unpoliceable territory, it might be imagined that cyber-criminals are simply operating in a zone they understand and are comfortable in, thus eliminating the borders defining 'real world' routine activity theory.

Familiar areas make the crimes of real-world offenders easier to commit (Potchak, McGloin and Zgoba, 2002 cited in Pizarro, Corsaro and Yu, 2007), thus the hypothesis of the digital arena as 'familiar area' may be further augmented by considering "ready to use software packages to automate cybercrime" (Hopkins and Dehghantanha, 2016, p. 23). Crime services such as automated spam email

(Kigoulis, 2017) and exploit kits (see Glossary) ensure that committing crime in cyberspace is easy for motivated criminals.

Demographic lifestyle (Tewksbury and Mustaine, 2003) and structure of routine activities can influence criminal opportunity (Cohen and Felson, 1979). Experiences created by and enhanced due to the internet may be different for each demographic, but the structure of user activity is likely to be similar and presumably based around personal communications and services. Hence, regular 'routine' internet activity may become hazardous, with potential for exploitation by motivated offenders (Arntfield, 2015). Cohen and Felson (1979, p. 589) implied that changes in routine activities may affect opportunity for the convergence of offender and target. The authors suggested that if the proportion of offenders and targets "in a community" (ibid., 1979, p. 589) remain constant, then a 'change' in routine activities may produce more incidences of victimisation. To position this in contemporary surroundings, consider Castells (2005) digitally networked society, as the 'community', where collaboration and interaction takes place. According to security literature (McAfee, 2018; Symantec, 2018; Symantec, 2019) offenders motivated by the facilities of electronic systems, and victims made suitable by reliance on digitisation are plentiful and thus constant. From an offender perspective, cyberspace is a "target-rich environment" (Hicks, 2018b) and **RQ1 actual/perceived risks** will consider digital reliance as a potential contributor to organisational risk. Constant suitable victims and numerous methods to exploit user activity and digital systems may be a factor motivating individuals to enter "deviant activity" (Lyng, 2005, p. 52). Thus, the "invitational edge" (Matza, 2010, p. 110) of the digital domain may continue to

entice prospective cyber-criminals to leap into deviance and “convert” (ibid., 2010 p. 119) into motivated offenders.

Therefore, the ‘change’ to increase incidences of victimisation (Cohen and Felson, 1979, p. 589) may be integration of an emerging technology and the anticipated benefit to society taking precedence over any potential threats (Hauptman and Sharan, 2013). Beck (1992) proposed that “risks and hazards” are “systematically produced as part of modernisation” (Beck, 1992, p. 20) and “hazardous side effects” (ibid., 1992, p. 20) are associated with the “normal operation of science and technology “(Kearnes, 2008, p. 123). To place contemporary ‘tech-driven’ culture against the backdrop of ‘reflexive modernity’ and the ‘risk society’ (Beck, 1992) in 2019, nine hundred and fifty million global users (950,000,000) used NFC (Near Field Communication) to make a point-of-sale purchase using their mobile device (Clement, 2019a). Two hundred and fifty thousand people (250,000) used a virtual reality application to view musical acts performing at a festival instead of attending in person (Evans, 2019). These statistics indicate that new technologies are implementing a ‘change’ in methods of paying for goods and services and participating in entertainment events. As “innovative technologies engender unexpected alternative futures” (Adam and van Loom, 2000, p. 8) and “major technological developments will give rise to new, unprecedented risks” (Beckstead et al., 2014, p. 3), more incidences of victimisation may be an “incidental problem” (Beck, 1992, p. 26) as users adopt new practices and each technological advancement introduces a change in routine activities.

As emerging technologies reach mainstream acceptance and are incorporated into daily use, the implication that demographic lifestyle might be an element in victimisation may prove to be a substantial observation (Tewksbury and Mustaine, 2003). The eighteen to thirty-four 'millennials' were the group to "lead contactless adoption" (Visa Europe, 2018, para. 1) and pushed the use of payments by tapping a debit or credit card against an NFC reader (ibid., 2018). Therefore, it might be assumed that younger demographics are amongst the pioneering early adopters who establish mainstream use of emerging technologies. This may have particular relevance now that the millennial age group are entering senior and executive positions in the work environment. It is anticipated that younger users as decision-makers will introduce increased mobile technologies to ensure efficient working in and out of the workplace (Whittle, 2020). As novel products emerge, digital natives may continue with early adoption and "thus embed a risk that is not qualified or clear to the average user" (Hicks, 2018b). Use of emerging technologies is relevant to both **RQ1 actual/perceived risks** and **RQ2 average usage/impact**.

2.5.2 Target Attractiveness

In traditional RAT, the motivated offender chooses a target who meets certain criteria of suitability. In the cyber domain an offender may derive suitability from observed internet behaviour and information available through active digital footprints. The fundamental difference is that online observation can take place from any location, and the offender need not be in close proximity to the target. No tracking technologies are necessary, as a criminal can easily monitor activity by observing any social media habits. For example, time and frequency of

posting, membership of groups or fora, and interaction with other users. Observation of activities may determine whether the target is suitable for social engineering, likely to respond to malware infected spam or other forms of targeted phishing. A target may be attractive due to status or relationship to another with rank or position, access to corporate data or administrator rights to a network and suitability derived via observable digital behaviour is relevant to **RQ1 actual/perceived risks**.

Cyber-RAT introduces a paradox where target suitability is not only determined *via* routine activity but *because of* routine activity. To place this in context, it must first be appreciated that malware and other automated crime services can be purchased from online marketplaces (Geier, 2011; Hurlburt, 2017; Tomazic and Vilela, 2017). These "bazaars, enabling easy purchase of illicit goods and services" (Shillito, 2019, p. 186) are located in an area of the internet referred to as the "dark web" (ibid., 2019, p. 186), regarded by the cyber security industry as "a breeding ground of cyber-crime" (Hurlburt, 2017, p. 102). The dark web should not be confused with the 'deep' web which is a moniker for unindexed web resources such as databases and public records only accessible by dynamic search techniques. The dark web is referred to as a "secretive, anonymous place where shadowy users access hidden services" (Bradbury, 2014, p. 14), where criminals converge on online fora (Leukfeldt, 2014) and phishing, spam, and hacking techniques (Chaudhry, 2017a) can be shared and sold. Access is not restricted, and a simple Google search will retrieve guidance to enter illicit marketplaces and access proxy servers to preserve anonymity (Tarquin, 2016). Typical entry uses a free browser available from the Tor Project (available at

https://www.torproject.org/). Initially intended to protect online privacy and circumvent censorship (Tor Project, 2020), Tor is recognised as facilitating access to the dark web (Lee, 2017) and hides a user's location by sending all internet traffic from the IP address through multiple servers and encrypting it three times (Tor Project, 2020).

Thus, a prospective attacker need not possess advanced technological skills as automated tools can install malware on thousands of computer systems (Caballero et al., 2011; Doshi, Athalye and Chien, 2010) to facilitate exploitation of software vulnerabilities (Palmer, 2020a). Consequently, multiple attacks taking place simultaneously relinquish an offender's control over target suitability. Any random user might become victim of a "self-propagating cyber weapon" (Thornton-Trump, 2018, p. 18) and being an active internet user may be the only requirement necessary to facilitate convergence with an offender or instrument to extend the reach of an offender (Hicks, 2018a). Target attractiveness is therefore established as a consequence of accessing the internet and a vulnerability to the exploit or attack method (Hicks, 2018b) and is relevant to **RQ1 actual/perceived risks**. In respect to user preference for internet access using mobile devices (Clement, 2020b) target attractiveness has relevance to **RQ2 average usage/impact**. As Internet of Things devices are connected to the internet and susceptible to online harms (see 3.11) attractiveness is a consideration for **RQ3 IoT unexplored risk**.

According to Roth and Roberts (2015), RAT is focused on *events*, rather than offenders, and crimes are facilitated by the absence of a guardian. Thus, the

concept of event-driven victimisation applies well to routine cyber activities. For example, a user may access the internet on a daily basis and follow a typical routine without incident. The user may make no deviation to customary activity, other than follow a link to a sensational news story, read an email sent by their bank, or click a hyperlink on a social network leading to a quiz offering a prize. Nonetheless, an innocuous *event* may allow malicious code to access the users' device or computer.

Internet risk can be exacerbated by simple user behaviours including 'carefree' browsing without attention to which sites are visited, clicking on hyperlinks without caution, and presumption that all content and emails are from legitimate sources. Criminals use tricks to fool users into assuming that what they encounter online is genuine (Microsoft, 2018). Hence, 'subconscious' cyber conduct may expose the user to an offender or instrument with no awareness that convergence has taken place and is relevant **RQ1 actual/perceived risks** and **RQ2 average usage/impact**. A user may not realise their device or system has been compromised until acquaintances complain about unusual activity originating from an email account or social media profile. This may be spam email received by all contacts stored in the users address book as a method of spreading malware (Landesman, 2018), or infected content posted to a compromised profile which 'tags' (adds a name or label) all the users' friends (Davis, 2018). A typical scenario is that the user has allowed malware to access their software or operating system by opening a phishing email, using unsecured software, or accessing compromised code (Grimes, 2017). Of the components which constitute traditional RAT, the absence of guardianship as the facilitator of crime

and victimisation is a vital element associated with risk in the cyber domain. Thus, cyber-RAT suggests that absent guardianship allowed the user to access the malware and failed to prevent the infected code from corrupting the user's system.

2.5.3 Capable Guardians in Cyberspace

Traditional RAT guardianship can be implemented by physical entities such as people and dogs, or by a proxy guardian, for example, a burglar alarm or close proximity to a neighbour (Hollis, Felson and Welsh, 2013). Similarly, cyber equivalents have multiple connotations and may be a physical or virtual human entity, or manifest as tools, settings, or controls. Hence, to prevent a compromised network, a guardian may be robust antivirus (AV) software. This 'tool' may have capacity to warn the user before they access a hazardous website and quarantine or delete infected code before damage is caused (TechTarget, 2002), thus preventing victimisation. Controls and settings available to enable privacy on social networks may also be regarded as guardians. Deliberately or inadvertently leaving privacy controls disabled and content without guardianship may allow the 'theft' of personal data and has relevance to **RQ1 actual/perceived risks**.

Those who assess workplace risk and prepare for unanticipated incidences may additionally be thought of as guardians, since failure to plan or prepare for the occasional unexpected incident may allow victimisation of a network to occur. In organisations where an IT (Information Technology) department has responsibility for software updates, antivirus upgrades and ensuring that networked computers or devices are safe to access corporate data, the department takes the role of

capable guardian. Now that mobile and cloud technologies have expanded the boundaries of the workplace, company servers can be accessed via an employee's own mobile device and employees need not be restricted to a desk or local network (see 3.5). In an organisation using cloud services, an IT department as guardian is now virtually obsolete (Bennett, 2016). It might therefore be argued that device manufacturers and software distributors should take responsibility for capable guardianship. To an extent, this takes place when security weaknesses are observed, and manufacturers respond with updates to operating systems. Nevertheless, the user is reliant on the response time of software vendors who react according to the severity of the security weakness (Temizkan et al., 2012), implying that there may be occasions when capability of guardianship is affected. Guardianship is a key element of the central investigation, and subsequently, absence of capable guardians has relevance to **RQ1 actual/perceived risks**; **RQ2 average usage/impact** and **RQ3 IoT unexplored risk**.

2.5.4 The Networked Society as Guardians

The harms that can be conducted via the internet are numerous and varied. Some are facilitated by technology, others by humans and many are a combination of both. Unlike crime in the physical world, a cybercriminal can "automate" victimisation and commit "thousands" of crimes with minimal effort (Mittal and Sharma, 2017, p. 1344). Thus, the argument that a capable guardian may prevent digital victimisation can be challenged. For example, Holt and Bossler (2008, p. 15) acknowledge that antivirus might act as ''general computer capable guardians" and protect a user from malware; but the authors argue that

AV solutions do not offer protection from malicious communications (Holt and Bossler, 2008, p. 6). This argument is technically correct, as harassment occurs as a result of complex human relationships and AV software alone cannot prevent malicious communications sent from one user to another. Nevertheless, this grievance may be re-evaluated in the broader context of guardianship, thus modifying the overall perspective.

Harassment using the internet as a delivery method can only occur if the victim is a participant in cyberspace. Hence, an individual receiving malicious web-based communications will be a member of the networked society. Throughout the vast network of communication platforms are innumerable users who act as 'gatekeepers' (Castells, 2011). These administrative and moderating guardians prevent unwanted participants accessing areas where users interact, for example groups on social media and online fora. The gatekeepers have capacity to remove users who prove undesirable or to prevent them from adding any content. The 'friends' in an individual's immediate social media network, and other vigilant users may all act as guardians and report unacceptable conduct. The networked society provides many guardianship services that a user can engage to prevent unwanted attention. These include 'blocking' to prevent communication from an undesirable participant, filters to stop emails, reporting abuse, and privacy controls. Cyber-RAT stipulates that the absence of a capable guardian facilitates victimisation, therefore, a user who continues to receive malicious communications may not have taken advantage of available guardianship. Despite this, it should be recognised that enabling cyber-guardians will not prevent harassment per se, only the virtual element will be guarded against. Real

world methods such as SMS (text messages) may continue to deliver malicious communications unless physical guardianship is enabled. In the example above, a real-world guardian to prevent SMS harassment may be activating controls to block a nuisance number.

To return to the theory that AV solutions do not defend against online harassment (Holt and Bossler, 2008, p. 6), it might be assumed that a cognisant user who acknowledges value in protecting a digital system may have awareness for self-protection. When viewed through the lens of cyber-RAT, a user proactive in making use of antivirus software may additionally have aptitude to report abuse, block others from networks and tighten personal privacy. AV software per se cannot protect against malicious communication yet might be considered as a member of a team of guardians, and consequently an arsenal of defences against online harms, of which malicious communications may be one.

2.5.5 Observed Guardianship

Guardianship in Action (GIA) (Reynald, 2009) demonstrated that capable guardianship is measurable by observing behaviours. Guardianship can be seen in operation when “availability, supervision and monitoring, and intervention activities” are in place (Hollis, Felson and Welsh, 2013, p. 72). Reynalds’ (2009) GIA related to physical properties, for example buildings, but when considering cyberspace, the property requiring protection is data. Ideally, any data the user has a responsibility for should be secured. This might include personal or sensitive data, digital assets and data pertaining to others which might be accessed via lapses in a users’ own security.

As an example of GIA in practice, the model can be applied to the premise of this research study. It is assumed that personal technologies will accompany employees into the workplace, thus indicators of GIA can be observed in the context of the organisation as guardian to protect employees and corporate data from victimisation. Hence “availability” (Hollis, Felson and Welsh, 2013, p. 72) might refer to accessible and robust anti-malware systems available for employees and provided free of charge by the employer. “Supervision and monitoring” (ibid., 2013, p. 72) may be procedures to ensure that employees protect personal devices, combined with emphasis on assisting average users to understand internet risk. Therefore, behaviour might be observed in provision of cyber awareness training which engages and educates. Antivirus software is the typical security solution available to average users, but security experts state that AV is not always effective against sophisticated code engineered to avoid detection (Ross, 2018). To supplement technical solutions, users may be taught to recognise the visual signs of a compromised system (Grimes, 2017) and subsequently “intervention activities” (Hollis, Felson and Welsh, 2013, p. 72) will be put into practice.

2.6 The Average User

Arntfield (2015, p. 379) suggests that applying RAT to the online environment “shifts partial responsibility for the occurrence of crime to its victims”. Despite the work of Arntfield (2015) relating to victims of cyber bullying, the author’s statement may also be applicable to average users of the internet. In the home environment, users are responsible for safeguarding personal devices, systems, and data. If an incident occurs which could not have happened if security controls

were enabled, the user who failed to implement appropriate measures will be held accountable. Likewise, if failure to maintain security of a personal device instigates a cyber incident in the corporate environment, some responsibility may also be attributed to the users' behaviour.

In an observation of characteristics, Rughiniş and Rughiniş (2014, p. 112) categorised users to examine how each group evaluated the risk of their routine online activity. Of the authors' classifications, the "economically rational" user is of interest (Rughiniş and Rughiniş, 2014, p. 112). This individual evaluates risk according to personal experience and adjusts their behaviour accordingly. If neither they, nor any acquaintance has been subjected to online victimisation, it is likely that these users assess the risk of internet harm as very low. Cyber awareness and corresponding protective actions are related to personal experience and "bound to a user's broader activities" (Rughiniş and Rughiniş, 2014, p. 113). Thus, "security measures are not justifiable per se" (ibid., 2014, p. 113), as the authors recognise that users equate technological risk to direct experiences of loss. If protective measures are only applied as a response to personal circumstance, then a user with no exposure to direct or indirect victimisation cannot wholly comprehend the necessity for robust cyber hygiene. Accordingly, this user may always remain in the position of suitable target and is relevant to **RQ1 actual/perceived risks**; **RQ2 average usage/impact** and **RQ3 IoT unexplored risk**.

If victims of online crime do indeed have partial responsibility for victimisation, then internet users may need to improve awareness so that a potential threat might be recognised and avoided. This researcher would therefore argue that

average users might be better equipped if they could appreciate risk on a more intimate level, by appreciating the correlation between lifestyle, personal use of technology and potential harm. Competent decision-making as a "reasonable response to recognised risks" may then occur, instead of "mechanically obeying external directives" (Rughiniş and Rughiniş, 2014, p. 113). Users may take advantage of the guardianship facilities of technology to protect data, devices, and systems, as the absence of any controls increases the opportunity for convergence with a criminal or instrument.

2.6.1 The User as Capable Guardian

The concept of the user-as-guardian can be explored by returning to Reynalds' (2009) theory of Guardianship in Action (see 2.5.5) where the role depends on a guardian being both available and capable of intervention. Reynald (2009, p. 4) considers that "intervention may be viewed as the ultimate act of guardianship". Hence, to apply GIA to the concept of user-as-guardian, consider an individual who has received bespoke training to recognise internet risk in a personal context, rather than a summary of generic cybercrime. An aware user has capacity for intervention, thus demonstrating that guardianship may be measured by the use of self-protective actions (Tewksbury and Mustaine, 2003). As a fortuitous default, a user-guardian will always be present when perusing the internet.

Hollis, Felson and Welsh (2013) claim that a target cannot be a guardian, particularly in the physical world. The authors define self-defence and guardianship as two distinct elements which must remain separate in order to retain "theoretical clarity" (Hollis, Felson and Welsh, 2013, p. 76). Even so,

guardianship as “the presence of a human element which acts – whether intentionally or not - to deter the would-be offender from committing a crime” (ibid., 2013, p. 76) can easily be transposed to cyberspace. An informed ‘human’ user may be proactive at managing risk presented by internet use and having achieved cognisance is unlikely to choose to resume position of vulnerable target. Ergo, such a user can only be a guardian, not only by application of personal awareness, but capacity to engage assistance of additional mechanical or physical guardians. Despite this, cognisance cannot remain constant in a society which demands continuous evolution of technology. A cycle exists where shifts in routine practices are instigated by new applications or enhanced devices. An “unwarranted faith in technology” (Hicks, 2018b) creates a lacuna where user guardianship is absent until threat of harm is confirmed, and methods established which may mitigate the risk. This suggests that training and awareness raising should be a continual process rather than a sporadic event, so that informed users might be capable guardians until the next cycle of emerging or disruptive technology. Nonetheless, despite a mindful users’ best intentions, unknown entities will always exist. Novel and sophisticated malware or particularly convincing social engineering can overcome capability and allow victimisation. Furthermore, there will undoubtedly be occasions where user-guardianship may be absent. Possibly by not engaging fully with security options through a desire for haste or lack of motivation. New and unfamiliar technologies may additionally result in diminished awareness. Hence, a user may still be a target, irrespective of their intrinsic or developmental capacity for guardianship and this is thus relevant to **RQ1 actual/perceived risks**; **RQ2 average usage/impact** and **RQ3 IoT unexplored risk**.

The following points may consolidate the user-guardian model. The one who owns a personal technology, and all associated software is ultimately responsible for guardianship. No other entity is obliged to ensure that a user's personal digital system is maintained with improved versions of software and applications. The user who neglects to respond to a manufacturer's security alert reduces capability as guardian during personal use (in addition to any networks they may be utilising). An evolving area of computer security and data protection is the concept of privacy enhancing technologies (PET). PET is an umbrella term used to describe any approaches, technological or otherwise, that may be used by an individual to protect personal data and online privacy (The Royal Society, 2019b). Thus, PET can include (amongst others) facilities to enable anonymous browsing, ephemeral communications which claim to automatically expire user-generated content (Office of the Privacy Commissioner of Canada, 2017, para. 5*)*, anonymising channels to disguise a users' IP address, such as the TOR network (Domingo-Ferrer and Blanco-Justicia, 2020, p. 284) (see 2.5.2), or even "a piece of tape masking a webcam" (The Royal Society, 2019b, p. 12). Privacy controls on social media are also an example of privacy enhancing technologies (Danesiz et al., 2014) and individual users have responsibility for activation and ensuring robustness by remaining vigilant to any modifications made by the social network. A user who leaves a personal profile in an unprotected state has missed an opportunity for safeguarding against inappropriate monitoring, theft of personal data and social engineering. Re-evaluating PET in the context of cyber-RAT places these technologies in the category of capable guardian and average users enabling PET as a measure to protect online privacy and (or) personal data may be seen as user-guardians. Ultimately, user guardianship may be defined as the

awareness for potential harm instigated by routine cyber activity and the protective actions initiated by that awareness. Thus, the user-as-guardian has significance to **RQ1 actual/perceived risks**; **RQ2 average usage/impact** and **RQ3 IoT unexplored risk**.

2.7 Cyber-RAT in Action

Despite the academic argument against routine activity theory as a model to explain cybercrime, this research proposes that certain elements may transfer to the digital environment. The following hypothetical example will combine components of traditional RAT to illustrate how a cyber-specific framework may be applied to a contemporary cyber scenario. An attacker may purchase automated crime services from the dark web (see 2.5.2) and send malicious spam emails to millions of email addresses stolen during data breaches (Hunt, 2017). The offender has no control over choice nor suitability of victim, nor any comprehension of whether capable guardians are present or absent. The attacker can only anticipate that eventually a suitable target will converge with the malware and victimisation will either be prevented by a guardian or will take place. In this example, the element that enables the crime is the routine activity of a user opening email. The motivated offender is the attacker who purchased malware and the instrument extending the reach of the attacker is the spam email. The random victim has the status of suitable target simply as a consequence of using the internet. The guardians are both the cyber awareness which alerts the user to avoid unsolicited email, and the antivirus software to prevent the malware from compromising the digital system. If guardians are present, victimisation is far less likely to occur.

2.7.1 Fluidity

An anomaly observed when viewing cyberspace through the lens of cyber-specific RAT, is the concept of ‘fluidity’ between target, offender, and guardian. The next hypothetical example will explain ‘fluidity’, using the context of this research study and a theorised attack instigated in the corporate environment. An employee enters the workplace with a smartphone used for internet activity in personal space, for example, the employee’s home, their commute to work or any opportunity where unrestricted internet usage might take place. Unbeknown to the employee, a malicious website installed malware whilst browsing. The employee uses the smartphone to share content with colleagues and the malware passes to other devices. The infected code is eventually shared with a colleague connected to the corporate network.

In this example, routine internet activity positions the employee as suitable target. Absence of cyber awareness or security controls allows victimisation to occur when the employee converges with the malicious instrument. By introducing the compromised device to the workplace, the employee becomes a conduit and takes the role of offender or extends the reach of an underlying motivated offender. The routine activity required during the average working day places the organisation in the position of suitable target. Absent guardians are the security controls, for example antivirus or updated software, on devices belonging to the colleagues who converge with the offender. The roles of target, offender and guardian were initially assumed by the employee, then by the colleagues whose devices spread the infection. In this hypothetical scenario, the outcome may be that the malware was detected and apprehended by the organisations cyber

security guardians before it corrupted the network. Alternatively, the malware might be a unique strain unidentifiable by the corporate antivirus mechanisms. In the absence of a guardian capable of prevention, the malware could traverse the network, infiltrate critical data, and compromise other connected devices. Thus, the organisation would then share the fluid roles of target, guardian and (unwitting) offender.

2.7.1.1 Physical and Virtual Offenders

Cyber-RAT further demonstrates 'fluidity' by suggesting that the motivated offender can include both physical and virtual entities. This concept is unfamiliar to traditional RAT where the assailant is typically human. In cyber offences the developer of malicious software, disseminator of infected code or creator of other instruments designed to cause harm may be a human entity. Likewise, a fake 'friend' on social media who conducts a social engineering attack or stalker sending malicious communications (McGrath and Casey, 2002) may be a physical being. A human is also likely to act as a sexual predator using social media or online games to 'groom' a victim (Cheong et al., 2015; Koch, 2008).

Using cyber-RAT as a framework, maliciously engineered code may also be seen as an assailant, or 'virtual offender' capable of convergence with a target. Thus, a fake website 'booby-trapped' with malware, a phishing email or an infected hyperlink might be considered as "offenders-in-technique" and "the conduits expressing the motivation of human offenders" (Hicks, 2018b). They execute an attack independently of the human entity and have the potential to converge with a target, regardless of physical or digital existence. A social network may be the

'perfect' conduit since the "default design…is exploited to conduct attacks and spread malware" (Sood and Enbody, 2011, p. 32). Thus, potential for infection is high due to the interrelationships between users. Social networks often have accompanying message services, for example, Facebook is associated with 'Messenger' and Instagram has 'Threads'. Hoax messages can be generated by what appears to be a legitimate service, to encourage users to access a website where malware is shared to their computer or device (Palmer, 2017a; Palmer, 2018a). Thus, an internet platform may also act as motivated offender-in-technique (Hicks, 2018b). The commonality seemingly shared by cyber and traditional RAT is that the offender, virtual or physical, is the recipient of the benefit of victimisation.

2.7.2 Fluidity and Liquid Modernity

The implication that a role defined in the physical world has a fluid existence in the cyber domain may be typical of "fluid modernity" (Bauman, 2000, p. 8) which suggested the "re-thinking of old concepts" defining the prior "solid" order of society (Bauman, 2000, p. 4). Recognising that fluids do "not keep to any shape for long and are constantly ready (and prone) to change it" (ibid., 2000, p. 2), the author proposed a "liquid modernity" (Bauman, 2000, p. 12) as the construct of contemporary society. Post-millennial civilization has (thus far) arrived at the point where mobile systems grant 'any-time, any-place' access to the digital domain and average users move fluidly between physical and virtual worlds, often inhabiting both simultaneously. As a very simple example, consider accessing social media or internet news resources whilst lying in bed. Progressive technologies and speed of connectivity have exacerbated an existence where

users can spend “twelve hours a day” viewing a screen “untethered from any sense of physical place” (Glancy, 2020, para. 9). Since the internet is “fleeting and volatile in its content” (Capeller, 2001, p. 233), the user can ‘flow’ seamlessly from page to profile to video, thus giving greater impact to the old-fashioned analogy of “surfing the internet” (Polly, 1992). Whatever the user accesses virtually, becomes their reality (Glancy, 2020, para. 9) and applies to content viewed on a smartphone screen, a games console or television providing on-demand streaming services. Hence, an internet-enabled ‘reality’ is not only dynamic and variable, but also easily malleable to personal taste. If viewed through a lens of liquidity, the ever-changing, never-ceasing existence of twenty-first century society may equate to a fluid reality.

Capeller (2001, p. 233) sums up the nature of the internet by describing it as “not centralised” and “constantly changing technologically” which compares well to the contemporary ‘tech’ driven ethos, where any ambitious software engineer can push new and untried technologies out to the global network of users. Nonetheless, the ‘always-on’ culture, twenty-four-hour access, and instant communication, combined with constant desire for the next ‘new’ thing can create a ‘viral’ sensation overnight to be forgotten and replaced within a week, a day, hours, or minutes. Even the ‘tech giants’ who facilitate the current modernity are in flux. Facebook is gradually being usurped by competitors (Hamilton, 2019) and may eventually join the list of once-familiar internet services no longer compatible with the taste of modern users (Hollingsworth, 2019).

Although published prior to the arrival of the social media era of Facebook, Instagram and other contemporaries who exacerbated the rise of the networked society (Castells, 2005), it may be considered that Bauman's (2000) theory was prophetic of internet-driven contemporary culture. If the "stable orientation points" by which one could "let oneself be guided" were in "increasingly short supply" (Bauman, 2000, p. 7) in the millennial year, they may be almost absent two decades later. Hence, the ongoing comparison of cyberspace to the 'wild west' (Hymas, 2020; Kounalakis, 2018; Look,1999) due to lack of "patterns, codes and rules" (Bauman, 2000, p. 7). If fluidity is already apparent, emerging technologies may remove any residual solidity. Goodwin (2016) advises that adjusting to the transition between virtual and physical space will challenge humanity, as "our sense of reality, of time and place will be the most complex for us to understand" (Goodwin, 2016, section 4). The author predicts that as a virtual life offers a safer, more comfortable, and intimate existence, society will increasingly choose a virtual reality over a physical one.

In the year 2000, Bauman observed that society was "moving from the era of pre-allocated reference groups" (Bauman, 2000, p.7) to a modernity with limited "systemic structure" and "unstructured, fluid state of life-politics" (ibid., 2000, p.8). Two decades later, the move towards an absolute virtuality is already evident. Integration between human and machine is enabled by embedding microchips into brains and bodies for healing and enhancement (Corbyn, 2019; Eadicicco, 2020; Odorčák, 2019; The Royal Society, 2019a). A seamless amalgamation of internet and brainstem may eventually eliminate the requirement for 'bridging' technologies such as virtual reality headsets. Fully digitised beings may herald an

end to the corporeal human presence in favour of an endless stream of real-time data. Thus, the notion theorised by the cyber-RAT framework that principal elements of RAT may flow to and from one other, is not inconceivable. Bauman's (2000) theory of liquid modernity has been briefly elaborated here as a theoretical exploration of the concept of fluidity in cyber-RAT. Readers wishing to know more may find the following works of interest: Garrett (2012); Huang and Tsao (2015) and Taranowicz (2018).

2.7.3 Control

Section 2.5.1 debated changes in routine digital activity brought about by integration of new technologies, in the context of *creating* more opportunity for the occurrence of crime. A contrasting perspective proposes that 'changes' in routine activity may have capacity to *reduce* the possibility of cybercriminal incidents. Cohen and Felson (1979, p. 589) suggest that if "controls through routine activity were to decrease" then crime would increase, advising that "control therefore becomes critical" (ibid., 1979, p. 589). If 'control' is placed under the umbrella of 'capable guardian' it may therefore be concluded that guardianship is key. As the internet is now deeply embedded in contemporary society and users are unlikely to withdraw from the digital environment, dependence on technical solutions as a method of 'control' may actually disempower the average user (Hicks, 2018b). An assumption of security may instead cause an undervaluing of risk and complacency during routine activity, thus instigating further opportunity for convergence with motivated offenders (ibid., 2018b). Therefore, to instigate positive change, every user may benefit from the capacity to control their personal cyber environment. Enhanced awareness and improved individual guardianship

may prompt subtle changes in routine behaviour, thus reducing occasions of suitable target, and subsequently diminishing opportunity for convergence.

2.7.4 A Theoretical Cyber-RAT Framework?

Table 2 (below) demonstrates the theoretical modelling proposed in this chapter.

Fundamental Elements of Cyber-Specific RAT					
Routine Digital Activity	**Target Attractiveness**	**Motivated Offender**	**Guardians**	**Virtual Space and Time**	**Fluid Roles**
Habitual **'day-to-day'** use of smartphones, tablets, laptops or desktop computers. Includes Internet Browsing, Downloading Apps, Social Media, Streaming, Gaming, Gambling, Communication (chat) Apps and other web-based activity.	**Selected Target.** Deliberately chosen for value in social engineering, i.e for job role or status in organisation, or key relationships. **Random Target.** A user becomes a suitable target due to presence in cyberspace and vulnerability to attack method.	**Physical (Human) Offender.** Methods may include: targeted social engineering (spear phishing), predatory activities (grooming), stalking, harassment, or malicious commmunications. **Virtual Offender.** Instrument or conduit to extend the reach of an attacker. E.g websites or hyperlinks infected with malicious code, phishing emails or malware masquerading as genuine apps or software.	**Physical Guardian.** 1. User as Guardian: cyber-aware, proactive with system/software updates & antivirus/privacy controls. 2. Risk-Manager as Guardian: empowers users with cyber awareness. 3. Organisation as Guardian: provides robust technological solutions. **Virtual Guardian.** Anti-virus and malware solutions, firewall, VPN, system/software/app updates, passwords, online resources, e.g privacy controls, blocking, reporting, gatekeepers.	**Space** is the internet location where convergence occurs of suitable target and offender (or conduit to extend reach of offender). E.g a social network profile, or web-based email account. **Time** is exact point during routine digital activity when convergence occurs, i.e an infected hyperlink is clicked, or phishing email opened. Target and Offender are not required to be present in cyberspace at the same time nor to share physical locality. Virtual space and time enable convergence.	1. **Target-to-Offender.** A device accessing the internet was Suitable Target and victimised by malware. Device is now Offender and a threat to networks and other devices. 2. **Target-to-Guardian.** A user accessing the internet is Suitable Target. The user is cyber-aware, enables antivirus, avoids suspicious content and becomes Guardian. 3. **Guardian-to-Target-to-Offender.** A corporation using robust security is Guardian and can prevent victimisation by malware. Employees wth poor cyber behaviour may position corporation as Suitable Target. If convergence occurs, coporation may become Offender to threaten others connected to the network.

Table 2, The Theoretical Cyber-RAT Framework

The reappraisal of traditional RAT to reflect a digital reality suggests a framework where target, offender and guardian may be considered in a cyber-specific context. Framing the research questions (see 1.2) in cyber-RAT demonstrates that the central investigation is driven by two essential epistemological queries. These may be summarised accordingly: how does an average user become a suitable target, and how does an average user become a capable guardian? (Hicks, 2020). The actual risk pursued by **RQ1 actual/perceived risks** is linked to potential convergence assisted by internet presence, digital footprints and enabled by absent guardianship. **RQ2 average usage/impact** is orientated towards recognising routine employee activity which may facilitate convergence through 'unsafe' use of technologies, or by user footprints enabling victimisation. The exploratory investigation of Internet of Things pertinent to **RQ3 IoT unexplored ris**k seeks unexplored routes to victimisation and applies the concept of guardianship to technologies vulnerable to virtual attack.

2.8 Conclusion to The Theoretical Framework for RAT in Cyberspace

Chapter Two methodically re-evaluated elements of 'real world' RAT to theoretically associate the traditional crime prevention theory with cyber-space, finding virtual equivalent to suitable target, motivated offender and capable guardian and substituting routine activity with habitual and regular *digital* activity (2.3). The chapter connects issues stemming from routine technology use to the research questions: suitable target in the context of **RQ1 actual/perceived risks** and **RQ2 average usage/impact** may arise from passive and active digital footprints (2.3.2, 2.3.3) generated during routine internet use. Suitable targets for random attack by virtue of presence online is contemplated in light of physical

offenders using virtual instruments to extend reach or act as conduit (2.5.2) and is relevant to **RQ1 actual/perceived risk.** Routine internet access using personal technologies associates random suitability with **RQ2 average usage/impact** and 'smart' Internet of Things devices accessing the online environment as suitable target are associated with **RQ3 IoT unexplored risk.** In common with 'real world' RAT, the absent guardian is a key element leading to convergence, and cyber-guardianship may be physical or virtual (2.5.3). Absence of capable guardians allowing event-driven convergence through random suitability has relevance to **RQ1 actual/perceived risks**; **RQ2 average usage/impact** and **RQ3 IoT unexplored risk**. The average user as absent user-guardian is likewise relevant to **RQ1 actual/perceived risk; RQ2 average usage/impact** and **RQ3 IoT unexplored risk.**

Chapter Two established the concept of RAT in cyberspace as the foundation underpinning the research study and offered visual interpretation to consolidate the model (Table 2, 2.7.4). The methods to be seen later in the methodology chapters (Chapter Four, 'The Corporate World'; Chapter Five, 'Executive Risk' and Chapter Six 'A New Direction') are guided by and enabled due to active and passive footprints left by average-user employees (see Table 1, 2.3). The reader may recognise cyber-RAT applied in the dual contexts of identifying a suitable data-subject for the research and a suitable target from the perspective of an attacker. The analysis in Chapters Seven, Eight and Nine applies the framework to theorise risk, identifying where technology use may position a user as suitable target and suggesting where guardianship might be enabled or enhanced. The forthcoming literature review (Chapter Three) evaluates technologies, devices and

internet harms in the context of suitable target, motivated offender and potential for convergence.

Chapter Three: Literature Review:

3.1 Introduction

This chapter will critically analyse literature evaluating threats to, and associated with, the average user during typical interaction with contemporary and emerging technologies including mobile (personal) devices and widely accepted internet platforms. An awareness of these potential harms is necessary to conceptualise application of cyber-RAT when considering target suitability, potential convergence, and opportunity for applied guardianship. To be technically correct, the 'internet' is the complex system of interconnected networks which support the environment accessible to users known as the World Wide Web or the Web (McGrath and Casey, 2002). Throughout the thesis, the online space is referred to as the digital domain, the internet, the virtual arena, cyberspace, or variations of all the above. For reasons of clarity, the reader may assume that the discussion refers to the Web, the environment accessible to users where typical activity occurs.

As a general observation, the language of computing is overtly technical and is particularly so for literature pertaining to cyber security and computing. Papers aimed primarily at the computer science academic or IT professional can be confounding to the layperson. For this reason, the literature review will endeavour to enlighten without bewildering. Readers may be familiar with the concept of cyber threat, but the magnitude of potential harm to internet connected devices may not have been thoroughly explored. Thus, the literature review will attempt to be accessible to generalist and specialist readers alike.

A generic issue observed throughout the study of technology and associated human behaviour is that sources cited in the literature quickly become dated. Historical works presenting an author's visionary theory will always have value, for example, Castells (2005) and the networked society, but technology does not remain static and instead constantly evolves. To place this in context, the 'smart' technologies discussed in 3.11 have advanced exponentially since the inception of this research project, compelling several updates to this literature review. Discussion of contemporary technology must incorporate topical themes, hence referencing reports produced by cyber security researchers is prevalent throughout academic work (Bertino and Islam, 2017; Britton, 2016; Chaudhry, 2017a; Fielding, 2020; Furnell and Clarke, 2012; McCusker, 2007; Tsai et al., 2016). Although not peer-reviewed academic research, security reports are of value to the social science researcher for they provide current information. Evolution of contemporary technologies, areas of concern to the cyber industry and methods of internet criminal activity are of particular relevance and this literature review will also cite security reports as a source of reference.

3.1.1 Chapter Arrangement

This review will comment specifically upon works relevant to users of personal technologies and of pertinence to the central investigation and the chapter is arranged as follows: Section 3.2 provides a brief overview of the response from the UK financial sector regarding the threat of cyber-attack against critical banking systems. Section 3.2.1 will critically assess the currently perceived view of organisational insider threat and 3.3 evaluates the modern internet criminal, instruments, tools, and common harms to which the average user may be

exposed during regular internet use. In 3.4, the literature assesses Web 2.0 and the potential for harm introduced by interactive 'social technologies'. Section 3.5 evaluates cloud services and 3.6 summarises the review thus far to clarify relevance to the research questions.

Literature relating to the mobile arena begins in 3.7 and the evaluation includes mobile devices, applications, associated malware, and vulnerabilities before the summary of relevance to **RQ1actual/perceived risks,** and **RQ2 average usage/impact** in 3.8. A new perspective of insider threat is proposed in 3.9 taking account of new technologies. The summary can be found in 3.10. The literature review will then discuss the Internet of Things (3.11) including 'smart' and wearable technologies, consumer devices and an evaluation of security risks. The summary relating the section to **RQ3 IoT unexplored risk** can be found in 3.12. Chapter Three closes with analysis (3.13) and conclusion (3.13.1). Throughout the chapter, any connection to a relevant research question will be indicated by referencing **RQ1actual/perceived risks**, **RQ2 average usage/impact** or **RQ3 IoT unexplored risk**.

3.2 Cyber Threat to the Financial Sector

The threat of cyber-attack to the financial industry and infrastructure is a key issue and the UK has a comprehensive range of cyber security measures in place (Cabinet Office, 2016; HM Government 2015). The Bank of England (BoE, 2015 p. 14) acknowledge cyber-attack as a serious threat, and to ensure that financial organisations maintain robust cyber resilience, CBEST security assessments were implemented (BoE, 2020, para. 8). As confirmed by the BoE, CBEST is a

brand for recognition purposes rather than an acronym that represents underlying words (Fisher, 2015, p.10; Hicks, 2018a). The CBEST system assesses “the people, process and technology that comprise a firms cyber security controls” (BoE, 2020, para. 8) and uses ethical hacking to infiltrate systems and services (BoE, 2016b). Unlike traditional emulated network assessments (Fisher, 2015, p. 9) and tabletop exercises (BoE, 2016b), a CBEST test examines live systems to identify any vulnerabilities creating risk (Fisher, 2015, p. 10).

A penetration test conducted using the CBEST framework is driven by threat intelligence bespoke to the organisation. The Bank of England advises that traditional methods of security testing are no longer adequate and organisational resilience should instead be grounded in knowledge. A greater understanding of “how”, “who” and “why” (BoE, 2016c, p. 4) will equip an organisation to defend against a “new breed of professional, sophisticated and industrialised threat actors” (ibid., 2016c, p. 4). An awareness of assailants who pose the greatest risk, and realistic attack methods which might be used against them are fundamental to organisational resilience (BoE, 2020, para. 8). Of equal importance is knowing where information about the organisation is available online as it might be exploited during an attack (ibid., 2020, para. 8). Certified security professionals subsequently conduct tests simulating attackers perceived by government agencies like GCHQ and other commercial threat intelligence services to be genuine threats (BoE, 2016c, p. 5). A CBEST test therefore empowers organisations to be responsive and proactive (BoE, 2016c, p. 5).

A requirement of the framework is “targeting” (BoE, 2016b, p. 16) where the “attack surface” (Digital Shadows, 2015, p. 4) is evaluated from the attacker's perspective in the manner of “threat actors as they prepare for their attack” (BoE, 2016b, p. 16). CBEST acknowledges that internal personnel may threaten organisational security (ibid, 2016b, p. 22) and the literature suggests a risk of phishing (Fisher, 2015, p. 2). Despite this, CBEST resources offer no further insight to the role of the employee, implying that threat intelligence focuses on attackers identified by external resources and insider risk appears to follow the model according to Mouton, Leenan and Venter (2016), Saxena et al. (2020) and Warkentin and Willison (2009) (see 3.2.1). Emphasis for organisational cyber security is predominantly on technology-based solutions (Colwill, 2009; BoE, 2016a; Salim and Madnick, 2014) and even the steps to organisational cyber security recommended by The National Cyber Security Centre are predominantly technological (NCSC, 2018a). The only inclusion of the human element suggests that staff should be trained to recognise any unusual activity as part of their role in assisting to keep the organisation secure (ibid, 2018a). Employee digital activity, personal technologies, and small-scale dynamic risk as a potential contributory factor to cybercrime is (apparently) not considered.

3.2.1 Perceived Insider Threat

An ‘insider’ is an individual with authorised, legitimate access to corporate data or information systems (Williams, 2008) and may be an employee, contractor, or partner (Saxena et al., 2020; Tyler, 2016). An insider may have access to the entire corporate network and could, through deliberate or indirect actions, cause severe harm (Warkentin and Willison, 2009, p. 102). Additionally, personnel might

be influenced by outsiders to disclose sensitive data, subsequently allowing unauthorised access to secure systems (Mouton, Leenan and Venter, 2016; Saxena et al., 2020). Insider threat may be summarised as 'malicious', 'compromised' or 'careless' (Saxena et al., 2020, p. 3) and is considered as the 'greatest' of all the risks to an organisation (Warkentin and Willison, 2009, p. 102). Regardless of the acknowledgement that the employee is the weakest link within a security system, corporate investment against insider threat is far lower than that for external threats (Colwill, 2009). Human assistance is essential for security as the threat landscape is too great to rely solely on technology (Furnell and Clarke, 2012). Despite this, those responsible for protecting corporate systems face the challenge of communicating the relevant issues to people who do not share the same perception of risk (Werlinger, Hawkey and Beznosov, 2009).

Non-compliance of information security policies has been much studied in a behavioural capacity, and the literature categorises insider threats as intention based or unintentional (Furnell and Clarke, 2009). Intentional threat can be defined as 'wilful, malicious violation' (Warkentin and Willison, 2009 p. 101). This may be associated with disgruntled or dissatisfied employees (Liang, Biros and Luse, 2016) or ex-personnel who have left an organisation with a resentful or vengeful attitude (United States Attorney's Office, 2015). Examples of intentional threat include: destruction or theft of data, leaking information to a third party (Punithavathani, et al., 2014), deliberate online publication of corporate data (Ring, 2015), or sabotage of work or IT systems. Insiders may also abuse knowledge of detection protocols and conceal intentional threat behaviours behind typical daily actions (AgrafIotis et al., 2015). Colwill (2009, p. 187) highlights how

a subverted or ‘placed’ insider, positioned by an external attacker is more cost-effective than an external attack. Consequently, attackers find it less challenging to gain access to a protected system through an individual, as emotion makes a human more vulnerable than a machine (Mouton et al., 2014, p. 267).

Examples of unintentional threat include poor password management or failure to log out of computers or workstations (Warkentin and Willison, 2009). Inadequate handling and destruction of sensitive materials or loss of a corporate device including mobile phones or laptops (Tyler, 2016). Additionally, accidental distribution of non-public information on public web servers, or sensitive data reaching incorrect recipients (Verizon, 2015, p. 49). Unintentional or accidental insider threats are often linked to poor training or lack of awareness and management support and system design may also be a factor in security failures (Kraemer, Carayon and Clem, 2009).

3.3 The Internet

This next section (3.3) begins the investigation to answer Research Question One (**RQ1 actual/perceived risk**) and identify *actual* risks created by insiders in the contemporary workplace. The discussion will commence with a brief overview of internet criminals in the contemporary digital age and a simple explanation of vulnerabilities in the context of computerised systems. This is followed by a thorough examination of the threats that users may be exposed to during normal interaction with the internet and web-based technologies.

3.3.1 Internet Criminals

Computer and cyber-criminal activities have been academically defined by categorising computer crime as an assault against machines and systems, and cybercrime as criminal acts committed through the use of a computer (Chik, 2007). Bartolacci et al. (2014) suggest that younger generations raised in a technological society may be more likely to commit internet crimes, given that their superior knowledge of technology places them in a position to facilitate abuse of systems. Nonetheless, youth may not be the determining factor. The online environment instils a perception of anonymity and combined with less visible social controls may encourage any user to deviate from socially acceptable behaviour (Kerstens and Jansen, 2016). The portrayal of a computer hacker as a social pariah in a darkened room surrounded by screens is the familiar image promoted by the media and creators of light entertainment. Instead, Xu, Hu, and Zhang (2013) argue that hackers evolved from intelligent, curious, exploratory students, intrigued by computers and their functionality, rather than socially inept delinquents. The motivations of a hacker should be considered differently from those of a criminal, for a hacker is interested in computers and networks, whilst computers are of interest to criminals only as a resource for nefarious activity (National Communications System, 2000). Hackers attempt to break into computer systems incited by several motivators, which may include peer prestige, notoriety, and the challenge of defeating complex security protected infrastructures (Matthews, 2016). Other provocations may be revenge or sabotage (Xu, Hu, and Zhang, 2013) or ideology induced hacktivism (Seebruck, 2015). In contrast, criminals are typically motivated by greed and the pursuit of financial gain (Grabosky, 2001; Horn, 2006; McCusker, 2007; Morris, 2004).

Security researchers equate the cybercriminal community to an industry which utilises professionals and organisations in a manner appropriate to a legitimate business sector (McAfee, 2008, p. 6; Symantec, 2016, p. 60). Criminals operating in the contemporary online environment may be part of an organised crime group (McCusker, 2007). This could be a structured group employing corrupt IT professionals, a wider network of criminals operating online and trading in digital properties (Broadhurst et al., 2014; Chaudhry, 2017a) or part of a global macro network filling 'structural holes' as required by the criminal activity (Spapens, 2010, p. 200). In the instance of cyber criminality, Broadhurst et al (2014, p. 3) suggest the 'structural holes' may be admittance to the "darknet and underground Tor sites" described in 2.5.2 and access to automated tools and resources developed and distributed by hackers (Chaudhry, 2017a; Shillito, 2019) enabling simultaneous attacks against thousands of computers.

3.3.2 Vulnerabilities and Malware

In computing, an error in the code or a flaw in the logic of an operating system, software or application (app) is known as a 'vulnerability' (Kaspersky, 2016). Vulnerabilities are created during product development and may be caused by several circumstances. These may include: lack of security within coding practices, use of open-source code, and components or factors within the threat environment which change after inception of the product and before completion ready for market (Veracode, 2016) (**RQ1 actual/perceived risks** and **RQ2 average usage/impact**). Due to the scale, complexity, and functionality of contemporary products, it is impossible for software to be developed which is free of errors (Kaspersky, 2016; Reis, Barth and Pizano, 2009; Zhang, Raghunathan

and Jha, 2014). The more software present on a digital system, the greater the probability of an "exploitable security vulnerability" (Rouse and Haughn, 2019, para. 3). Manufacturers typically have no initial knowledge of the vulnerabilities in their products, but once a flaw has been detected, it is a potential access point into a computerised system. The product is thus exposed to potential criminal exploitation until new software is developed to update and 'patch' the fault (SentinelOne, 2016) (**RQ1 actual/perceived risks** and **RQ2 average usage/impact**).

A vulnerability can be found in almost any kind of software, and from the perspective of an attacker, a popular and widely accepted program is the most attractive target (Symantec, 2016, p. 5). Internet Explorer, Adobe, Microsoft Windows and Office (Symantec, 2015, p. 38) are extensively used by both consumers and professionals and often contain vulnerabilities (**RQ1 actual/perceived risks**). When a software manufacturer is made aware of a security hole, a solution will be developed and distributed swiftly, at which point the end-user becomes responsible for updating their system. This again offers examples of guardianship in the context of routine activity theory. The manufacturer is responsible for the production of the updated software to repair the vulnerability. The user must respond to notifications about installing updates. Until the system is updated, the software and the user are exposed to possible attack (Amirtha, 2016) (**RQ1 actual/perceived risks** and **RQ2 average usage/impact**). Thus, a delay in response by the software vendor (Temizkan et al., 2012) or failure by the user to update promptly creates absence of guardians and victimisation may occur.

A ‘zero-day’ vulnerability is a security flaw with exceptional value to internet offenders as manufacturers, developers and users have no knowledge that it exists (Techopedia Securities Institute, 2017). The vulnerability is named in response to the number of days a security patch has been issued to repair it, hence, ‘zero-day’ as no security solution is available (Porup, 2019). Zero-day vulnerabilities are typically “accidental bugs” (Lohn, 2018, para. 1) which may take “hours, weeks or months of painstaking effort” searching through lines of code to find (Singh, Joshi and Kanellopoulos, 2019, p. 164). The finder can sell the exploit to a broker who will then sell it on for the best price (Porup, 2019; Singh, Joshi and Kanellopoulos, 2019, p. 164). Zero-days to be used against the Windows operating system have sold for two hundred thousand dollars ($200,000 USD) (Cimpanu, 2019a) and those enabling specific attacks against the Apple iPhone may fetch up to a million dollars ($1,000,000 USD) or more (Porup, 2019). A zero-day has such value because they are “the most difficult attacks to defend” (Lohn, 2018, para. 1) and can defeat “traditional defences” (Singh, Joshi and Kanellopoulos, 2019, p. 164). Consequently, an attacker using an unknown flaw to access a network may remain undiscovered and cause considerable damage (ibid., 2019, p. 164). Locating and trading in zero-day vulnerabilities is a lucrative profession for internet criminals (Cimpanu, 2019a; Frei, 2014; Paganini, 2016; Symantec, 2016).

Offenders use ‘instruments’ to enhance their attack capacity (see 2.5.2). The primary example of an instrument is malicious software (malware) used to exploit an unpatched vulnerability and gain access to a system (PC Tools, 2016). Malware is the generic name for any software or program with “mischievous

intention” (Qamar, Karim and Chang, 2019, p. 888) specifically engineered to cause harmful impact to computers, mobile devices, or network performance. Common examples are worms, Trojans, spyware, and rootkits (Razak et al., 2016). A popular method of exploit is for a Trojan program disguised as legitimate software to enter the computer system through a security hole. The malware will then modify the users’ internet browser settings to the least secure option, thus allowing more Trojan programs to be downloaded from the internet (Kaspersky, 2016; Symantec, 2016b) (**RQ1 actual/perceived risks** and **RQ2 average usage/impact**).

Some malware can replicate and spread, hence, if infected code has successfully compromised a computer system, it may be passed to other users on a network or via communication methods such as Bluetooth (Kan, 2020; Puranik, 2019), SMS (text) and chat/messaging applications (Osborne, 2020). Blended threats mix features from different varieties of malware families to create multiple attack vectors (TechTarget, 2005) As an example, the infection may be introduced via email, spread infected code throughout the network and download other Trojan programs from the internet to create a backdoor entrance into the user's system. Polymorphic malware has been augmented by the developer to constantly alter the appearance of code to evade detection by protection mechanisms (Drew, Hahsler and Moore, 2017). This “stealth technique” (Masabo et al., 2018, p. 1763) allows the malware to mutate, forming new variants which present a new identity for each attack “without changing the body of the virus” (ibid., 2018, p. 1762). ‘Zero-day’ malware is unknown malicious code which traditional security solutions such as antivirus, intrusion detection or intrusion prevention cannot

recognise (Gupta and Rani, 2018, p. 104). Zero-day malware is engineered to circumvent detection systems (Tran et al., 2016) and attackers are constantly creating new malware samples and advancing techniques to “fool the detectors” and by-pass security systems (Gupta and Rani, 2018, p. 104). Ninety-three percent (93%) of malware seen by security researchers in 2018 was observed to be polymorphic (Webroot, 2019).

Malware engineers design software to perform certain functions or achieve specific goals (Razak et al., 2016), most often financial gain (SentinelOne, 2016), and will typically target systems with the greatest number of users. Once a new application or programme gains popularity, it will become more susceptible to attack. Productivity applications (SentinelOne, 2016) are a typical target, particularly Microsoft Office programmes and PDF readers due to their widespread use by business sectors and home users alike. Attackers infect the distributors website with malware (Symantec, 2018, p. 28) and users are duped into installing a compromised update (Invision, 2019) (**RQ1 actual/perceived risks** and **RQ2 average usage/impact**). Vulnerabilities affecting software manufactured by Microsoft, Apple, Oracle, and Adobe are available for hire or purchase from markets located on the dark web (Kaspersky, 2016). Offenders may also take advantage of a vulnerability to gain access to a computer network without infecting it with malware. The objective is to alter system files and gain administrator or super-user status. Malicious activity, data harvest, or theft of intellectual property can then take place undetected, whilst the attacker conceals evidence of their actions (Thrive Networks, 2011) (**RQ1 actual/perceived risks** and **RQ2 average usage/impact**).

Web browsers such as Internet Explorer, Chrome, and Firefox among others, may also contain errors and flaws within the code. These vulnerabilities may expose users to attacks from the internet, simply by engaging in routine activities including viewing web pages (Bandhakavi et al., 2011; Greene, 2013). The average user may innocently use an old version of their favoured browser, unaware that security holes patched by newer versions are unrepaired in the software they are using (Reis, Barth, and Pizano, 2009). Browser vulnerabilities leave a user open to attack from human offenders and instruments in the form of websites compromised with malicious code, or websites which are fake or 'spoof' (**RQ1 actual/perceived risks** and **RQ2 average usage/impact**). Malware can harvest bank account numbers, passwords, and personal identification credentials from compromised computers. A network of infected computers disrupted by police in 2014 had already incurred losses of over one hundred million dollars using this method (FBI, 2014). Personal data is a valuable commodity which can be used for fraud or ID theft, and even old data has value for social engineering purposes (Rizzo, 2016). This is an example of an absent guardian facilitating victimisation, but even a cyber-aware user may not appreciate the necessity to update a web browser. Dormant guardians occur across the internet, but average users may not know of their existence. This thus corresponds with the recommendation that individuals should have capacity to make competent decisions as a response to recognised risk (Rughiniş and Rughiniş, 2014).

3.4 Web 2.0 Technology

Web 2.0 is the umbrella term for online technologies which enable users to interact by adding comments and uploading audio, video, text, and images for

others to remark upon and share. Examples of Web 2.0 include social media platforms Facebook, Twitter, Instagram, and LinkedIn, all renowned for the creation of user-generated content. Social networking involves connecting with others to create a social circle and socialise by sharing content or participating in other forms of online interaction such as chatting or playing games. Social networks are considered to be valuable communication tools which enable socialisation regardless of locality (Matook, Cummings and Bala, 2015). Consequently, social media is popular with cybercriminals who exploit networked communities by spreading scams, fake website links and phishing exploits (Symantec, 2016, p. 29) (**RQ1 actual/perceived risks** and **RQ2 average usage/impact)**.

The literature identifies narcissistic traits amongst ardent Web 2.0 users (Bergman et al, 2011; Carpenter, 2012), and digital narcissism has evolved from the constant urge for users to update and modify their profiles (Lovink and Rossiter, 2009). The current obsession indicating narcissistic behaviour is the production, enhancement and manipulation of images featuring food, travel, experiences, and most commonly, self-portraits (selfies). New images are posted regularly, intended for perusal by an online audience in expectation of positive and flattering feedback (Wang, 2017) (**RQ2 average usage/impact**). Personal data and images obtained from user-generated content on social media may be utilised by criminals gathering intelligence for identity fraud (BBC News, 2016) or social engineering (Gulenko, 2013; Hadnagy, 2010; Wilcox and Bhattacharya, 2020) (**RQ1 actual/perceived risks** and **RQ2 average usage/impact**).

3.4.1 Social Engineering

The key to successful social engineering is the exploitation of trust. Not limited to trust between humans but also trust in social networks (Mansfield-Devine, 2008). Social engineering takes place when an attacker uses “social interaction” to persuade (Mouton et al., 2014, p. 269) or manipulate (Wilcox and Bhattacharya, 2020, para. 2) an entity to comply with a specific request or perform a particular task. A simple example is the exploitation of personal content on a social media profile to convince a user of a ‘real world’ connection. By claiming familiarity with the target and their ‘close social network’, the attacker will gain trust (Tsikerdekis and Zeadally, 2014 p. 75), and a request to become social media ‘friends’ is more likely to achieve a positive response. Since the virtual environment encourages a rapid development of trust due to the “disinhibiting effect” of the internet, this may eventually lead to “increased online self-disclosure’ (Mesch, 2012, p. 1472). Users who maintain a large network and habitually use Facebook are most likely to accept unsolicited friend requests and subsequently succumb to phishing attacks on social media (Vishwanath, 2015) (**RQ1 actual/perceived risks; RQ2 average usage/impact**).

Prior to a successful social engineering attack, a threat actor must obtain intelligence about the target(s). Individuals may have no concept of the quantity of information available about them online (Hadnagy, 2010) nor comprehend the type of information an attacker would find useful (Junger, Montoya and Overink, 2017). Mesch (2012, p. 1471) suggests that a user’s “identifiability level” is a conscious decision resulting from details connecting a virtual identity with a real one. Nonetheless, regardless of any attempt by a user to preserve privacy,

tenacious open-source research can locate exploitable intelligence. Freely accessible public records, combined with monitoring online activity, may allow an attacker to obtain data about a target's home life, family, employment, organisation, colleagues, workplace and working hours (**RQ1 actual/perceived risks**).

3.4.2 Phishing and Targeted Attacks

Phishing is a common social engineering attack, designed to persuade a victim to divulge sensitive information or access infected code concealed within an unsolicited email. Known as a 'semantic' attack, a language-based method will target the user rather than the computer system (Mayhorn et al., 2015). An attacker will typically use 'urgent' language to encourage the user to act in haste, without taking time to review the message and ensure credibility (KnowBe4, 2017) (**RQ1 actual/perceived risks**). Examples are scam emails declaring an online account has been compromised and the recipient must respond 'immediately' to prevent further harm. Phishing attacks are "deliberately titled to exploit human behaviour" (PwC, 2018, p. 11) and criminals seek "hot topics" to attract attention and "hook" vulnerable users (Emm, 2020, para. 7). A phishing campaign may be directed at thousands of users, whilst relying on convincing social engineering to succeed. A popular tactic is to use branding to imitate correspondence sent from a Microsoft Office 365 account to convince users to open the email (Fireeye, 2019, p. 5) and Office documents and Windows apps are used to deliver the malware (Verizon, 2020, p.18). If the attachment needs Microsoft Office to open, a vulnerability within the programme will be exploited (Symantec, 2016). In 2019,

security researchers observed that forty-five percent of malware utilised Microsoft Office as a delivery method (Crane, 2020).

Security experts advise that contemporary cyber criminals employ a targeted approach requiring less assaults and achieving more success (Webroot, 2020, p. 7) and targeted attacks have been observed as a principal method against corporations (Symantec, 2019, p. 49). Victims are selected for the position they hold in the company or the value of information they have access to (Burns, Johnson and Caputo, 2019). Thus, s*pear* phishing differs from generic "wide-net" phishing (Burns, Johnson and Caputo, 2019, p. 25) by specifically focusing on one or more individuals purposefully selected as suitable targets. An email sent to spear phish a target will often exploit a 'zero-day' vulnerability (Symantec, 2016 p. 40) as organisational security mechanisms may fail to identify unknown malicious code (see 3.3.2). The risk of opening unsolicited email attachments is well documented, but a compelling and credible charade by a skilled social engineer may still dupe a target with good cyber awareness (**RQ1 actual/perceived risks**). Data extracted from social networking sites significantly improves the success of a phishing email (Jagati et al., 2007, p. 97). As examples, photographs might be copied from profiles in the targets network (Huber et al., 2010, p. 1) or relationships, common interests and "circles of friends" (Jagati et al., 2007, p. 96) exploited to convince the target of authenticity. As Symantec specify (2016, p. 6 and p. 41), attackers need only succeed once, and a successful targeted attack might infect the entire corporate network.

Other spear phishing methods involve convincing the target that a hyperlink to a useful web resource has been sent by a credible source. The link will then direct the user to a fake or compromised website where attackers attempt to obtain sensitive data (KnowBe4, 2017) or malicious code is downloaded to the computer system (**RQ1 actual/perceived risks** and **RQ2 average usage/impact**). Social engineering succeeds because the human quality of trust is exploited (Hadnagy, 2010) thus a user with an active social media presence may unwittingly provide the instrument of attack (**RQ1 actual/perceived risks**). The "defence against phishing attacks relies on humans, as well as technology" (PwC, 2018, p. 11) and is another example of potential for enabled guardianship. A cognisant user may guard against semantic attacks and antivirus and anti-malware technologies provide guardianship if the user-guardian is absent. Security research reveals that attacks instigated by spear phishing emails were conducted by sixty-five percent of cyber-criminal groups in 2018 (Symantec, 2019, p. 49). Evaluating this statistic using cyber-RAT suggests that motivated offenders are converging with suitable targets and capable guardianship is lacking.

3.4.3 Frauds, Spam, Hoaxes, and Malware

For a scam to succeed, it will require user interaction as the content must be distributed manually (Symantec, 2016). The design of a social media platform ensures that users share content, hence a social network is an ideal location for such activity to take place (Sood and Enbody, 2011). Many frauds and hoaxes will abuse a brand name or logo to appear legitimate and bogus content will offer gifts or access to media files as an enticement for users to make initial interaction. The fraud then requires users to 'share' or 'like', thus spreading the scam

throughout their network (Christenson, 2003). Users who succumb to a scam often give away personal details which result in identity fraud (BBC News, 2016) or an influx of spam email containing malware (**RQ1 actual/perceived risks**).

Offenders take advantage of real-life human-interest stories to create dramatic or shocking content to entice users to share with their network of friends and associates. Sensational news items can contain hidden threats known as clickjacking ('click' hijacking) or likejacking ('like' hijacking). These threats trick the user into remarking on fake content, with the consequences varying from spam to monetary theft or identity fraud (Dharmavaron, 2015). Fraudulent profile pages may generate content to mimic real users, yet the account can contain embedded links to phishing pages (Adewole et al., 2017) (**RQ1 actual/perceived risks**). Compromised social media accounts and associated passwords can be purchased from illicit marketplaces found on the dark web (Ashok, 2016) (see 2.5.2). Attackers will then exploit the trust between the legitimate user and their connections by distributing spam, phishing links (Ruan et al., 2016) or malware disguised as "hilarious or sensationalistic video" (McMillan, 2010, para. 2) (**RQ1 actual/perceived risks** and **RQ2 average usage/impact**). The "interconnectivity" between users (Sood and Enbody, 2011, p. 31) facilitates "chain infection" (ibid., 2011, p. 32) and the authors suggest that "it is not possible for attackers to spread malware directly, but they play around with the psychology of legitimate users to exploit users' ignorance" (Sood and Enbody, 2011, p. 33). When evaluating social media through the lens of cyber-RAT, social networks may be thought of as conduits to express the motivation of a human motivated offender (Hicks, 2018b) (see 2.7.1.1). All users frequenting social networks, even

those with guardians enabled by privacy controls may be suitable targets. Hence, the capability to prevent convergence may be a cognisant user-guardian or a suite of robust security solutions.

'Koobface' is sophisticated malware which has challenged security professionals since 2008. Described as a "complex system which preys on social networking sites" (Thomas and Nichol, 2010, p. 64), the malware generates scams which compromise user accounts by infecting a computer with harmful code. The code attacks the Windows operating system (Varsanov, 2016) and the infected computer joins a web of compromised machines known as a Botnet (a *net*work of ro*bot* machines). The computer can then be operated by a third-party controller (Anagnostopoulos, Kambourakis, and Gritzalis, 2015; Enisa, 2012) and used to create further fraudulent accounts to befriend victims and continue the cycle of infection. Bots can effectively imitate humans (Symantec, 2016); therefore, users should always exercise caution when accepting unsolicited 'friend' requests (**RQ1 actual/perceived risks** and **RQ2 average usage/impact**).

3.5 Cloud Services

Many organisations have switched to cloud-based business services for the convenience of Infrastructure as a Service (IaaS) and Software as a Service (SaaS). For the business sector, cloud computing is a more economical option for a corporation than maintaining in-house servers. Cloud providers take responsibility for the infrastructure, and data storage can be purchased on an ad-hoc basis, dependent on requirement. The concept of cloud computing may be of little interest to the average user, but routine internet activity may involve

interaction with the technology more than the user realises. Social network platforms, content sharing and popular messaging services, for example, Facebook, YouTube, WhatsApp, and Facebook Messenger are all cloud services. In addition, web-based email clients Gmail and Yahoo are examples of cloud computing. In principle, any fully functional internet service that can be accessed from any internet connected location is likely to be a cloud service. Popular activities for cloud users include social media, content viewing, collaboration gaming and media streaming.

Drobox and Amazon Cloud Drive are popular cloud-based content management sites. Users can upload large data files to be stored by the platform and other users can access or share the data. Nonetheless, file sharing sites are not immune to hacking attacks or malware (Gibbs, 2016; Wagenseil, 2013) (**RQ1 actual/perceived risks** and **RQ2 average usage/impact**). Chaudhry (2017a) suggests that use of online file sharing systems may be in decline, possibly because contemporary mobile and desktop operating systems provide access to cloud storage as a standard facility. This offers benefit to the user as data need not be stored on an internal hard drive, nor on external mechanisms like USB storage or optical devices (Tanasychuk, 2016). Content can be accessed from any web-enabled device and may be shared with trusted others. Nevertheless, the user should exercise caution when storing sensitive data in the cloud. Hacking exploits have proved that passwords protecting client accounts have been compromised with ease by criminals (Ashford, 2014; Kelion, 2014) (**RQ1 actual/perceived risks** and **RQ2 average usage/impact**).

Content sharing systems known collectively as Cyberlockers (Gil, 2016) have gained notoriety for illicit trade in illegal content (Chaudhry, 2017a; Daryabar et al., 2016; Fan, 2015). Users visit these sites with the intention to access pirated material. Examples of copyright protected content which has been illegally obtained are films still on theatrical release, music and other media unavailable through normative channels. Cyberlocker sites are renowned for spreading malware through compromised files (Netnames, No Date) (**RQ1 actual/perceived risks** and **RQ2 average usage/impact**).

Cloud services are accessed via the internet and are therefore susceptible to any vulnerabilities affecting the web. Hence, they are a potential security risk. The nature of cloud computing requires that content and data may be widely dispersed rather than confined to a single data centre. This factor, combined with the absence of physical hardware, entails difficulty in applying normative controls for cryptography and strong authentication (GroBauer, Walloschek, and Stöcker, 2011) (**RQ1 actual/perceived risks** and **RQ2 average usage/impact**). When choosing cloud applications, users do not typically consider security as a high priority. Analysis of twenty applications favoured by consumers revealed that only one app employed “enterprise-grade security controls” (Skyhigh Network, 2016, p. 25). Cloud apps contain many potential security flaws, including poor programming language (Long, 2015) or vulnerabilities allowing access to identified malware attacks (Johnson, 2016). In addition, business cloud apps are failing to meet industry standard compliance mechanisms (Johnson, 2016) (**RQ1 actual/perceived risks** and **RQ2 average usage/impact**). Other security risks introduced by placing corporate data onto a cloud platform include the risk of

personnel victimisation by a phishing or social engineering attack (Lastline, 2019). A corporate cloud resource can be accessed from anywhere, and once an employee's access credentials are obtained; the data is accessible.

3.6 Summary of 3.3 to 3.5 in Relation to Research Questions One and Two

Research Question **RQ1** seeks to understand the actual rather than the perceived risks created by personnel within a financial organisation. It is apparent from the literature that the infrastructure of all computerised systems and devices may be flawed from the development stage onward. It is not possible to create software free from errors, and digital systems may have multiple layers where vulnerabilities could potentially exist. These can include the operating system, software, and web and cloud access. If a digital system is connected to the internet, any errors and flaws in the code can be exploited by attackers. Malware can be introduced into the system, or the vulnerability used as an access point to enter a network. The literature highlights how popular software is a soft target for criminals who create malware specifically to target vulnerabilities present in programs and applications. Widely utilised software is likely to be found on workplace computers due to familiarity, function, and ease of use. Therefore, in relation to **RQ1 actual/perceived risks**, any member of the corporate workforce interacting with an internet connected computerised system is a risk. The risk is exacerbated if the system has commonplace productivity software installed.

The literature indicates that an active internet presence may provide material which can be used for social engineering. Even a cautious individual may unknowingly provide sufficient data for a skilled attacker to compile a convincing

email and implement a successful phishing campaign. Therefore, in relation to actual risk, employees using Web 2.0 technologies and divulging personal or sensitive information using their own identity may be a liability. The literature explains how scams and malware can be deliberately or inadvertently shared amongst social networks. An employee who is an ardent Web 2.0 user with many followers or friends, is more likely to involuntarily access malicious content which may ultimately threaten the IT network. A cyber-aware user may still be duped by an email or other content which appears to have come from a trusted or credible source. According to the literature, cloud applications may contain security flaws, are vulnerable to hacking attacks and might be responsible for spreading malware. Hence, in the context of **RQ1 actual/perceived risks**, the actual risk is created by employees who use cloud applications for content management, sharing or communication as part of their daily work routine.

Research Question **RQ2** examines how an employee may use their own mobile device and the potential impact this could have on the corporate IT infrastructure. The literature indicates that every web-enabled device is reliant on complex and sophisticated code. There is a high probability that a smartphone, tablet, or laptop, will contain some errors or flaws within the operating code, and it is plausible that many end-users will be exposed to vulnerabilities. A primary feature of portable devices is the facility for a user to install applications of their own choice. Thus, each additional application or program may add new security weaknesses from badly written code or might introduce malware created specifically to target mobile operating systems.

Web-enabled devices allow internet access from any location, depending on connectivity options. In the context of **RQ2 average usage/impact, an** average user accessing the internet for regular, everyday activity may unwittingly introduce malware into their device. Exposure may occur via web browsers or accidental access to code deliberately placed on websites; malware may be shared through infected content or via unsecured access points. An individual or organisation need not be intended as a target but may instead be a victim of random attack, as the contemporary internet criminal is indiscriminate, with access to an arsenal of malicious resources.

Any user of the internet will engage with Web 2.0 technologies in some capacity, for they are an integral part of the contemporary technological environment. In relation to **RQ2 average usage/impact**, users are choosing to conduct internet activity using web-enabled mobile devices. Social networks can be accessed using a smartphone or tablet and profiles updated throughout the day. Mobile applications for social media sites enable a photograph taken using the camera on a device to be uploaded immediately to a profile page, thus contributing to the sensitive data which may enable social engineering. Unless the geolocation service is disabled, a device will add the user's current location to any images produced. Hence, mobile-generated content may have added value for an attacker who can use internet resources such as Google Maps to identify where an image was created. Malicious content shared amongst social networks may infect a device if inadvertently downloaded by a user responding to fake news or a fraud. Any social media, messaging or downloading of content using an unsecured or compromised cloud-based application, for instance, Facebook,

Twitter, WhatsApp, or messenger, might expose a device to malware. When considering the impact, as suggested by **RQ2 average usage/impact**, a compromised phone, tablet or laptop brought into the workplace and allowed to connect to either the network or to other devices may spread malicious code throughout the entire system.

3.7 Mobile Internet Access

Government strategies and initiatives have focused on solutions for digital inclusion (Government Digital Inclusion Strategy, 2014) to ensure that the internet is available to all. Projects encouraging older people to embrace social media have reduced social isolation (Neild et al., 2014) and the World Wide Web Consortium (W3C, 2008) produce developer guidelines to ensure that web content is accessible to disabled people. Fifty-nine percent of the global population are active internet users (Clement, 2020a) and fifty-two percent of web content is accessed by mobile devices (Clement, 2020b). The concept of the internet transforming society from spatial, social interaction to that of online networks is becoming a reality (Castells, 2001) and personal technologies are the favoured method of internet access. Modern devices are designed to satisfy personal requirement and are lightweight with variable screen size. Smartphones, iPads, netbooks, MacBook's and laptops are attractive and competitively priced and operating systems are easily navigable. Tablets are intuitive and particularly easy for older people to use (Morris, 2014). Most importantly, such devices enable internet access from any location and do not confine the user to a desk.

3.7.1 Mobile Operating Systems: Android and Apple

Historically, the Apple operating system (iOS) has been regarded as the most secure. Stringent protocols are placed upon applications available for download, and Apple retains control over hardware, software, and firmware (Forrest, 2016). Developers observe strict regulations and Apple reserve the right to reject any applications. Software which had been previously available can be discarded, and an 'app' may be removed from an app store if Apple consider it is not functioning as expected, is outdated or does not meet the criteria set for developers (Apple, 2021). The secure status of the iOS is a cause of conflict for some Apple users, who would prefer greater flexibility and personal choice regarding software installation. Consequently, 'jailbreaking' an iPhone is a common practice. This involves installing tools and software from the internet to exploit a security vulnerability in the operating system allowing the manufacturer's restrictions to be removed (The iPhonewiki, 2015). The user can then modify the iPhone to their preference. As an example, the browser and default email service can be changed to one of personal choice and third-party apps unapproved by Apple may be downloaded (Hoffman, 2013). A device 'hacked' by jailbreaking loses security layers intended for protection, thus attackers can introduce malware, viruses or other harms and the device becomes an increased security risk (Apple Inc, 2018) (**RQ1 actual/perceived risks** and **RQ2 average usage/impact**).

In contrast, the Android operating system is designed to enhance the user experience by allowing applications and software created by open-source developers. Stringent control measures do not restrict the Android user, but despite this, some individuals prefer complete autonomy over their device and

perform an operation called ‘rooting’. This process grants ‘super-user’ access to the operating system, permitting alterations to the function of the device and allowing the user to remove all the excess software known as ‘bloatware’ (Hildenbrand, 2016). An Android device is already a vulnerable system due to the flexibility with applications (Murdock, 2016) and tools to execute rooting may contain malware when downloaded from the internet (ibid., 2016). Rooting a device may prevent it from receiving updates (Sinicki, 2019) and a user must then be proactive about obtaining security patches. Any installed applications with unpatched vulnerabilities will leave the device exposed. (**RQ1 actual/perceived risks** and **RQ2 average usage/impact)**.

3.7.2 Vulnerabilities and Malware for Mobile Systems

As with all computerised systems, flaws or errors in code or logic are present in operating systems and applications designed for mobile devices (**RQ1 actual/perceived risks** and **RQ2 average usage/impact**). Some mobile app developers use pre-written code from ‘software libraries’ to provide the functionality required for their apps, yet these code components have been known to contain vulnerabilities (Shaikh, 2019). Raghuramu et al. (2016) examined two million cellular network devices and known security threats and observed threats in zero-point seventeen percent (0.17%) of devices. Recent statistics show that global smart phone users now number three point five billion (Statista, 2020a) therefore, extrapolating the zero-point seventeen percent (0.17%) may imply that almost six million smartphones might contain security threats. This estimation does not take into consideration other cellular network devices, for example,

tablets and laptops (**RQ1 actual/perceived risks** and **RQ2 average usage/impact**).

The results published by Raghuramu et al (2016) may be usurped by contemporary statistics, since cyber researchers suggest that one in thirty-six mobile devices has “high risk apps installed” (Symantec, 2019, p. 41) (**RQ1 actual/perceived risks** and **RQ2 average usage/impact**). Both Android and iOS have proved vulnerable to remote attacks (Verizon, 2015, p. 19) (**RQ1 actual/perceived risks** and **RQ2 average usage/impact**). Vulnerabilities discovered in the Android operating system might allow an attacker to take control of a device if the victim opened an infected multimedia or MP3 file (Symantec, 2015, p. 12). The primary target for malware is the ‘endpoint’, for that is where sensitive data can be located (SentinelOne, 2016). When considering that mobile devices are used for banking, shopping, and other monetary transactions, endpoints may contain sensitive login details, access to accounts or passwords. Pop-up windows in web browsers frequently offer to remember log in details or passwords as a time-saving option for the user. Stored data of this nature can be harvested by malicious code and passed to a third party for unauthorised access. Sensitive data could also be personally identifying information accessible within social media accounts or emails (**RQ1 actual/perceived risks** and **RQ2 average usage/impact**).

Malware engineered for mobile devices may affect normal function of a device, bypass the access controls, harvest sensitive data, harass the user with unwanted advertising or assume control of a device without user awareness (Qamar, Karim

and Chang, 2019, p. 888). Malicious code disguised as legitimate apps are a growing threat (McAfee, 2019; Symantec, 2016), exacerbated by a trend for some malware applications to 're-invent' themselves adding to functionality and capacity to steal data (Emm, 2020). Since the rise in popularity of mobile banking apps, malware to target payment data and access credentials has increased (Checkpoint, 2019, p. 7). Like many other criminal tools, "malware builders" are available for purchase on the dark web (see 2.5.2) allowing "massive distribution" of new versions of banking malware by anyone willing to make the investment (Checkpoint, 2019, p. 7). Unlike those available for Apple devices, Android does not have stringent controls in place and developers of any level of experience or integrity may produce apps available for download. Nonetheless, despite due diligence by Apple, developers writing applications for iOS were attacked by malware which was later identified in the newly developed software (Symantec, 2016, p.8). Nine families of iOS threats have been identified where vulnerabilities might install malware on an Apple device (Symantec, 2015). More recently, iOS devices have proved vulnerable to attack from iOS specific zero-day malware (Goodin, 2019), websites infected with malware (Golubev, 2019) and surveillance malware (Whittacker, 2019).

Qian et al. (2015) reviewed security for five hundred and seventy-seven (577) popular applications, each with over one million (1,000,000) downloads. Findings revealed that three hundred and seventy-five (375) apps contained at least one vulnerability. Extrapolating this data suggests that three hundred and seventy-five million (375,000,000) users may have a vulnerability in their digital system (**RQ2 average usage/impact**). A recent development in the mobile threat landscape is

malware employing techniques to evade detection, including malware not acting maliciously if it detects it is being monitored (Bello and Pistoia, 2018) and delayed execution of the infected code to avoid detection in secure environments. Other techniques include encryption (Checkpoint, 2019) of the malicious payload (see Glossary). Furthermore, malware exists which is resistant to removal, reinstalling itself after the device is reset to the default factory setting (Cimpanu, 2019b) (**RQ1 actual/perceived risks** and **RQ2 average usage/impact**).

Threat intelligence reveals that cross-over threats are prevalent when users browse an app store using a remote computer system, for example, a desktop PC or laptop and download applications onto one or more portable device(s) (Symantec, 2016, p. 11). The 'cross-over' takes place when malware already present on the computer steals cookies placed on the web browser allowing the malware to impersonate the user and install malicious apps to their device(s). Users with a substantial number of applications may not recognise ones they did not personally select and is an example of absent guardianship allowing victimisation to occur, as unsolicited downloads might be malware in disguise.

3.7.3 Mobile Device Security

Mobile devices are regularly upgraded by users to take advantage of faster processing speed for seamless transitions between applications, and instant download of web content and media. High speeds require superior processing power, and software designed to protect devices may impede the operating system of a phone or tablet. Thus, despite the availability of antivirus solutions, users may choose to forgo them due to the risk of diminished performance

(Zhang, Raghunathan, and Jha, 2014) (**RQ2 average usage/impact**). Users may also decline to install antivirus on mobile devices as they assume that they do not visit websites or conduct activity which might place them at risk from online menace. Nonetheless, every web enabled device is vulnerable to threats from the internet (**RQ1 actual/perceived risks** and **RQ2 average usage/impact**). Malware designed to infect mobile devices may also be introduced via Bluetooth (Symantec, 2015 p. 19), text message (Symantec, 2015, p. 25) email and social media and can then propagate to other devices after infection (Chen et al, 2015). (**RQ1 actual/perceived risks** and **RQ2 average usage/impact**).

Given the expansion of malware deliberately targeted at mobile devices (Nokia, 2016), security may be considered paramount. Manufacturers are responsible for delivering notifications when improvements to their software are available, but the user may not be made aware of it immediately (Symantec, 2015, p. 12). Ideally, the user should be proactive about security, regularly maintain all installed applications and respond swiftly to any alert appearing on their device relating to a system update. This has relevance, for the literature states that the rate at which patches are produced is dependent on the type of vulnerability being patched. Those that impact on confidentially and integrity take precedence over others (Temizkan et al., 2012, p. 307). Therefore, if updates already delayed by software manufacturers are further postponed by users, mobile devices may experience periods where security is lacking. To place this in the context of cyber-RAT, unpatched vulnerabilities create absent guardians, and might permit the convergence between target and offender.

The price, availability and suitability for a particular device to a specific task entails that many individuals own and operate more than one mobile device. With many units and services at their disposal, users must make more security decisions and home users may be more exposed than corporate employees protected by sophisticated organisational security systems (Furnell and Clarke, 2012). For low income or large households containing multiple devices, costly superior antivirus may not be a high priority (**RQ1 actual/perceived risks** and **RQ2 average usage/impact**). Thus**,** publishers or vendors of applications should play a more significant role in detecting malware and vulnerabilities and remove responsibility from the user (Zhang, Raghunathan and Jha, 2014). In response to the proliferation of compromised applications, Google has taken measures to eradicate malicious apps found in online stores and enable automatic security updates. Additionally, Apple is concentrating on improving encryption services (Forrest, 2016). A further solution might be installation of robust antivirus software at the manufacturing stage, which would activate automatically when using the device for the first time. Security solutions should then remain free, and the onus should not be on the user to purchase or subscribe.

3.7.4 Bring Your Own Device

Cloud services have enabled the transition from logging into a work-based server to a virtual desktop and employees can now access work services from anywhere with available internet connection, including public transport and coffee shops offering wireless connectivity (Wi-Fi). The culture of Bring Your Own Device (BYOD) has become a necessity in the workplace as employees enjoy the flexibility of remote working. BYOD is permitted as an addition to the working

environment and a method of reducing company costs (Utter and Rea, 2015; Walker-Osborn et al., 2013). An employee may prefer to use their own device if it is superior to the tools offered by their employer (Ellis, Saret, and Weed, 2012), or prevents being confined to a desk or workstation. A device purchased by an employee may be more comfortable, with ergonomic design, and the user may be more confident with the technology, for example, the intuitive, heuristic touch screen interface (Park, Kim, and Ohm, 2014). Employees using privately owned devices may subsequently be more productive.

The security risks of BYOD are well-documented (Rivera et al., 2013; Zahadat et al, 2015) but the literature tends to focus on protection of corporate data. In particular, employees retrieving company files using potentially unsecured access to the internet, for example, public Wi-Fi spots (Russell, 2016). Security researchers advocate monitoring of devices accessing the network, use of management software to control data and bespoke protection per the type of data. Ideally, every request to connect to the corporate network should be assessed accordingly (Russell, 2016). Regardless of any BYOD policies and data protection protocols in place, a corporation should continue to assume that privately owned devices are an uncontrolled risk. Users may neglect security precautions (Symantec, 2015, p. 8) or avoid antivirus solutions (Chen et al., 2015 p. 194). Typical everyday internet use can expose a device to complex security risks including infected code, suspect applications (Paullet and Pinchot, 2014; Shabtai et al., 2014) or internet protocol vulnerabilities (GroBauer, Walloschek, and Stöcker, 2011). Content downloaded to a device by 4G (fourth generation of wireless mobile technology) could contain malware and the new 5G (fifth

generation) networks may facilitate faster downloading of numerous harms, including malware and other attack methods (Khan et al., 2019). As an effort to protect corporate data, an organisation may restrict employee access rights, yet users may still use devices to retrieve internal email, modify calendars and utilise corporate applications (**RQ1 actual/perceived risks** and **RQ2 average usage/impact**).

3.8 Summary of 3.7 in Relation to Research Questions One and Two

Research Question **RQ1** seeks actual risks, rather than those perceived to be associated with corporate personnel. Evidence shows that the internet is ubiquitous across the developed nations and all citizens are encouraged to use the web to access services no longer available offline. Portable devices allow connection from any location, thus internet access via a mobile device is steadily increasing. Many forms of device are available, and all use software and applications susceptible to vulnerabilities, malware, and internet harms. Despite efforts from manufacturers to protect the security of devices, criminals are developing new families of malicious code designed to target mobile operating systems. The infected code can be disguised as legitimate applications or hidden on the internet and accessed through everyday activity.

Organisations may permit BYOD and allow privately owned devices to be used for work purposes with appropriate policies in place, yet in relation to **RQ1 actual/ perceived risks**, there may be unconsidered hazards. Personnel may be denied access to corporate data yet might utilise compromised devices to access work tools or share files with other colleagues. Alternatively, undisclosed personal

devices may be present in the work environment. The literature identifies that malware and threats spread from the internet may be passed to other devices via other channels, therefore any portable device which has been used to access the internet is an unexplored risk.

RQ2 average usage/impact queries the usage of an employee-owned mobile device and the possible impact to corporate IT infrastructure. A smartphone owned by a user with advanced technological ability may be augmented to perform in a manner to suit the individual. Installation of unregulated applications can increase the risk of exposure to malware created to exploit mobile operating systems. Devices may have been used for illicit activity on areas of the internet renowned for spreading malware. An organisation permitting BYOD for work-based activity may not realise a device with an increased security risk is connecting to the IT network or accessing corporate data. The user may be insufficiently cyber aware to realise that their internet activity has increased the security risk of their device. Hence, it is important to understand what a device brought into the workspace has been used for as individuals may not apply protective measures.

Pre-installed antivirus software would remove the option for the user to decline protective measures to preserve processing speed, but devices pre-installed with superior protection would most likely increase in price. The added expense may prohibit some users, leading them to obtain cheaper unprotected models. Those who value processing speed may also purchase unprotected devices. In addition, users who prefer choice and control over their devices might modify the device to

suit, rendering the operating system vulnerable or exposing the device to applications downloaded from the internet which may be infected with malware. At present, a user has the choice to not install antivirus solutions on their mobile device in favour of speedy performance. A user might choose to delay installing updates to personal software and applications until the time is more convenient. A user may even choose to deactivate security defences installed in an operating system so that a device can be personalised and improved to a personal preference. Seen through the lens of cyber-RAT, these actions signify a calculated absence of guardianship and a deliberate facilitation of potential convergence with an offender or instrument. In relevance to **RQ2 average usage/impact**, a user who conducts internet activity on a knowingly compromised system and then brings the device into the corporate workspace, might be regarded as a motivated offender.

3.9 Insider Threat: A New Perspective

Any organisation using computerised systems will most likely employ protective measures to protect infrastructure and corporate data. Despite this, the cybersecurity industry acknowledges successful cyber-attacks where end-user participation enabled data breach or attack (Symantec, 2015, p. 79; Symantec, 2019; Verizon, 2015, p. 14; Verizon, 2020, p. 53). This suggests that users may be non-compliant of security protocols and (in)directly exacerbating cybercrime. Average users may be unknowingly engaging in (in)appropriate cyber behaviour, inside the business environment and in personal space. Factors may be ignorance and lack of cyber awareness, lack of competence with digital systems or indifference to technological risk (**RQ1 actual/perceived risks**). Evolution of

technology may alter a corporate environment, for example, when digital systems are updated or augmented to improve performance or service delivery. Adjusting to change when new technologies are introduced at a rapid pace may be overwhelming for both humans and social institutions (Orman, 2013).

The concept of humans overwhelmed by technological changes can be explored by examining Wi-Fi, Bluetooth, RFID (Radio Frequency Identification) and NFC (Near Field Communication). These recent technologies are ubiquitous in the contemporary environment and Wi-Fi, Bluetooth, and NFC is standard in modern mobile devices. Orman (2013, p. 25) implied that if many new technologies are introduced in succession, then risk can occur to society, concurring with Beck (1992) and the inevitable side-effect of technological modernisation. To place this in context for the average user, Wi-Fi and Bluetooth can spread malware, NFC payment systems can expose sensitive data (Nearfieldcommunication.org, 2017) or can be used to plant malware (Cimpanu, 2019c) (**RQ1 actual/perceived risks** and **RQ2 average usage/impact**). Individuals may not understand the technology they use, therefore cannot relate to the threats they are exposed to (Furnell and Clarke, 2012, p. 984) (**RQ1 actual/perceived risks** and **RQ2 average usage/impact**).

3.9.1 Too Many Threats – Not Enough Awareness

In 2016, a job vacancy on a recruitment website implied that the newly appointed information security manager would be expected to facilitate a cyber education and risk awareness programme. The job description declared that the role would include “chasing us up to complete the e-learning you sent us” (Bond Dickinson,

2016). This content, published on behalf of a corporation, suggests that employees do not engage with training and risk awareness provided by their employers. Some literature (Furnell and Clarke, 2009; PwC, 2018; Warkentin and Willison, 2009) endorses training and development as key to improving end-user compliance. Nevertheless, if instruction fails to engage, personnel may not be sufficiently motivated to attend sessions (Mayhorn et al., 2015). This is particularly relevant if the training is conducted online (e-learning), and the organisation relies on the individual to be proactive in their learning requirements (**RQ1 actual/perceived risks**). Delivery can be as important as content and individuals have different learning styles. Some favour personal interaction or lectures and younger people (apparently) prefer on-screen methods (Humphries, 2015). Training conducted by IT technicians may be too technical for those who are technophobic, conversely, such elementary training may not be interesting for those who are technically minded (**RQ1 actual/perceived risks**).

Cyber awareness is complex. The internet offers multiple aspects to threaten a user, and often threats are not from outside attackers but from the user themselves. Verizon (2020, p. 48) state the importance for each user to understand that they may be a potential target, particularly for social engineering. Silic and Back (2016, p. 39) explored how employees can become victims of phishing and identified a lack of training and awareness of the risks associated with social networking. Research demonstrated that training employees to recognise phishing emails can have varied success (Aburrous et al., 2010) although studies conducted in a ‘real world’ corporate environment may have more impact (Kumaraguru et al., 2008). The National Cyber Security Centre

advocates regular ‘refresher’ training to ensure that end-users within an organisation (employees) are familiar with the risks to the organisation they work for (NCSC, 2018b).

Even after training, users may still succumb to phishing, although more than one training session gives greater success (Kumaraguru et al., 2009) (**RQ1 actual/perceived risks**). Individuals with some degree of technical expertise may recognise the well-publicised dangers of poor cyber practice and attempt to protect themselves using security software and secure passwords. Despite this, the UK Cyber Defence Strategy (HM Government, 2016, p. 22) highlights how the public is “insufficiently cyber aware”. The strategy recommends that all users should understand how exposed they are on the internet (**RQ1 actual/perceived risks**) and correlates with the concept of capable guardian (see 2.5.3). An informed user who can make competent responses to recognised risks has personal ability obtained through awareness, and capacity to augment capability by enlisting assistance from other physical and digital guardians. To achieve awareness, recognising vulnerability during personal internet use and familiarity with the expanding range of innovative internet threats is beneficial. Security measures have no value unless the user can place them into personal context (Rughiniş and Rughiniş, 2014) hence a user lacking knowledge to equate routine activities with risk may always be in the position of suitable target.

3.9.2 Employees and Corporate Systems

When an organisation introduces new technologies into the IT infrastructure, the attack surface expands (Symantec, 2018, p. 38). Moreover, the increase in

threats may be more than the consequence of extra layers of potentially vulnerable software or operating systems. On each occurrence of a technological change, employees operating the system should be advised accordingly. As an example, an employee at a service desk in a high-street bank complained that the computer network in her branch is regularly updated. On every occasion, elements of the operating programme are modified and each time a change occurs, the staff do not know how to use the system (Anonymous, 2016). Employees unable to operate familiar systems can cause delays, frustration and eventually mistakes (**RQ1 actual/perceived risks).** Therefore, the example described above is indicative of a communication failure between front line and upper-level personnel.

Kraemer, Carayon and Clem (2009) identified that managerial support is instrumental to successful security. Salim and Madnick (2014, p. 2) advocate a systemic approach to treat the IT infrastructure as a whole, rather than a series of components, emphasising that people and management must be an essential part of any holistic security measures. The sentiment is echoed by Wilcox and Bhattacharya (2020, p. 1), who suggest that any holistic framework for security should include technical, procedural and user-centric controls.

Organisational security systems may project a false sense of safety to employees, who believe that a company firewall and antivirus will safeguard their online behaviour. Thus, they may assume that they have no need of vigilance during interaction with the internet. Similarly, users accessing the internet using a portable device connected to the company network may rely on organisational security to provide safeguarding measures. It is possible that company policy

requires systems to be configured to prevent access to certain online platforms, including shopping sites or social media. Hence, users may assume any accessible content is permitted and therefore protected. (**RQ1 actual/perceived risks** and **RQ2 average usage/impact**).

Furnell and Clarke (2012, p. 2) identify how an employee in a contemporary corporation may now be responsible for the operation of security mechanisms which historically would have been managed by a system administrator. This could include updating programs and applications and back-up of system files. The authors state that usability of security technology may play a significant role in non-compliance. Software interface and performance alongside cognitive tasks required by the user will all affect ease of use. An average user may be expected to perform tasks using complex systems or software they do not understand, therefore any errors made may not be recognised (**RQ1 actual/perceived risks**).

3.9.3 Bring Your Own Multiple Devices

The personal computer (PC) was created with the aim of allowing every person access to a digital system, but in current society there are now many computers per person (Alpaydin, 2016). This may be because personal mobile technology has limitations, and no single device suits all purposes. Some units are more appropriate to certain tasks due to screen size, text input or processing speed. With a myriad of available designs and a competitive price range, an individual might own and utilise several devices. For example, a smartphone for communication, a tablet with a larger screen for viewing multimedia files and a laptop with a keyboard to produce text documents. Contemporary employees

might bring more than one privately-owned device into the corporate environment, each one requiring access to the network. In addition, undisclosed web-enabled devices may be entering the workspace concealed in bags, briefcases, or pockets (**RQ2 average usage/impact**).

An organisation permitting BYOD is likely to have security policies and protocols which employees will agree to comply with. Nonetheless, a device owner who purchases their own data connectivity may expect less restriction regarding the personal use of their privately-owned devices (Ellis, Saret and Weed, 2012) (**RQ2 average usage/impact**). This expectation may then influence utilisation of devices during work hours in addition to personal environments and owners may assume unrestricted choice over applications and internet activities. Thus, devices may be used for gambling, social discovery or networking, dating, media streaming, multi-player gaming, or for viewing illicit content or adult websites (**RQ1 actual/perceived risks** and **RQ2 average usage/impact**).

Applications to enhance mobile internet experience (Hoehle and Venkatesh, 2015) and a cornucopia of utility and time-saving applications may be downloaded to devices, but internet trends can change rapidly. Online platforms, communication channels and popular apps fluctuate in popularity, and devices may eventually retain redundant, outdated software no longer supported by manufacturers or no longer updated by the user (ibid., 2015) (**RQ1 actual/perceived risks** and **RQ2 average usage/impact**). Users of privately owned devices make personal decisions about the software and applications they install on devices. They may choose to download open-source software and

updates to popular programmes, but these can be targets for criminals who conceal malware in the code (Symantec, 2016; Symantec, 2019, p. 17) (**RQ2 average usage/impact**). Chaudhry (2017a) discusses how a highly anticipated game was created specifically for mobile devices and launched with limited availability. When supply ran out within weeks, criminals took the opportunity to offer illegal downloads infected with malware. "Cracked" or "patched" games are known distribution methods (McAfee, 2020; Perekalin, 2019) and pirated copyright-protected media files may be downloaded from illicit sites where malware is distributed with the content (Batt, 2019; Daryabar et al., 2016; Fan, 2015; Paganini, 2019) (**RQ2 average usage/impact**). Copyright protected content and malware distribution is discussed further at 7.4.4.

Employees in the workplace may assume that internet browsing, social media or accessing applications on a personal device using 4G or 5G connectivity will comply with any company protocols regarding internet use. Average users may not comprehend that a device need not be connected to a network as malware can be spread through text message and Bluetooth (Jackson and Creese, 2012; Paullet and Pinchot, 2014) (**RQ2 average usage/impact**). Organisations may enforce strict rules to protect corporate data and restrict work activities on personal mobile devices. Despite this, Ellis, Saret and Weed (2012) identified that employees often perform unapproved work on their own devices. Absalom (2015, p. 16) noted that if an individual owns a smartphone, they will "highly likely" use it for work purposes. The author observed how the number of employees "actually" using personal devices for work, greatly exceeded the amount "perceived" by enterprise IT services (ibid., 2015, p. 24). Employees utilising BYOD may store

company data on multiple devices, making data protection policies more difficult to comply with (Clarke, 2016). Additionally, important data may be found in unusual places due to employees making copies of documents to work on elsewhere, thus exposing data to risk (ibid., 2016) (**RQ2 average usage/impact**).

3.9.4 Social Media and Mobile Social Networking

Social media has expanded beyond the original remit as a social networking tool and created a range of facilities specifically for the business sector. Experts predict that social media will become a platform where users can continue conducting activities without logging off or navigating away from the site (Mintel Group Ltd, 2016b). As an example, Facebook targeted the business market with a suite of collaboration tools, intended to connect all personnel within a corporation and "transcend language and time zone differences" (Codorniou, quoted in Brown, 2016, p. 1). Social media in the workplace has value for enabling collaboration in dynamic and decentralised workplaces (Forsgren and Byström, 2018) but as a work tool may encourage employees to maintain access to social platforms at all times. Previously, organisations may have controlled the use of social media in the workplace, using policies and systems configured to prevent access. Adoption of social networks in a business context may relax those protocols and allow work-time access to previously restricted sites.

There are estimated to be three point eight-one billion (3,810,000,000) active social media users globally (Statista, 2020b) implying that eighty-three percent of all internet users take part (in some respect) in social networking. A motivational factor urging users to conduct continuous inspection of social media feeds is Fear

of Missing Out (FOMO). Described as a user's concern that social media friends are having experiences from which they are absent (Przybylski et al., 2013) FOMO "pushes" users to remain in contact with one another (Yin et al., 2015, p. 268). The conviction that something more interesting is taking place elsewhere provokes regular monitoring and individuals receive alerts from social networking sites to remain up to date when content is posted. This frequently results in failure to maintain undivided attention (Harari, 2017) and coincides with suggestions that employees spend so much time checking devices that workplace productivity is affected (Stubbington, 2017). Since average users have approximately eight social media accounts (Kemp, 2020) and ninety-nine percent of social media users conduct their activity using mobile devices (Statista, 2020b) the observation that employees are "routinely sneaking lengthy peeks at their social media" (Stubbington, 2017, para. 2) may be valid. As an added consequence, and relevant to **RQ2 average usage/impact**, regular access of social media in the workplace may exacerbate the possibility of victimisation.

Wang (2017) discusses how social media narcissism involves posting photographs onto profiles, and the author identifies how desire to observe whether posts have been liked or remarked upon incites the user to check for updates. Female users post the most selfies on social media (Ormerod, 2018) and the proliferation of physically enhanced, provocative images have been found to be an indicator of social climbing, prevalent amongst women of lower economic status (Blake et al., 2018). This suggests that women compete against other women in a "complex social and evolutionary game" (Blake, 2018, quoted by Dubach, 2018, para. 13). Parker (quoted by Lanier, 2018) claims that social

media is an addiction where people become accustomed to the ‘dopamine hit’ that occurs whenever a photograph or post receives a comment or ‘like’. This is particularly relevant for the posting of self-portraits (selfies) for these are intended to invoke response and the narcissistic user is likely to be regularly seeking favourable reaction. Users become fixated upon what other people think, thus, people who receive positive acknowledgement form the habit of posting more content so that they can continue to receive responses. According to Lanier (2018), this modification of a users’ behaviour takes advantage of a weakness in human psychology (Parker, quoted in Lanier, 2018).

Self-absorption regarding responses to personal content may also apply to a users’ urge to witness how the online audience reacts when comments have been added to another person’s content. The desire to see whether a remark has been shared, ‘retweeted’ or considered ‘influential’ (Ormerod, 2018) may necessitate continual inspection of feeds, particularly if the user has a profile on many platforms. Seventy-eight percent of Facebook users access the social network using a mobile phone (Clement, 2020c). Therefore, notwithstanding any company policies restricting social media use, it is possible that privately owned portable devices are used within the workplace to access social networks (**RQ1 actual/perceived risks** and **RQ2 average usage/impact).** Social media is known to be rife with malicious content (see 3.4), and “exploitation of online social trust is considered an entry point of malware infections” (Sood and Enbody, 2011, p. 32). Thus, an employee eager for audience reaction who accesses social networks within company premises might be considered a risk (**RQ1 actual/perceived risks** and **RQ2 average usage/impact**).

3.9.5 Employees: Generational Differences

Digital natives or ‘millennials’ aged between eighteen and thirty-four (Gottfried and Dost, 2015) are renowned for their intuitive aptitude for computing and internet trends. This generation experienced new technologies as they emerged and have no concept of a society without networked systems. Individuals born before the digital revolution may also be highly proficient with specific interests or hobbies advancing their technical knowledge and ability. Social media has created a vast market for personal promotion and users may create videos, multimedia files, or video logs (vlogs). Avid smartphone users may perform operations to override manufacturer control. Other individuals may have coding, app development or website creation skills or an interest in testing the boundaries of security features in software. Game players may be familiar with ‘jailbreaking’ games consoles to make modifications (Xbox JailbreakTeam, 2017) (**RQ1 actual/perceived risks**).

Within the corporate workplace, millennial employees are encouraged to engage in reverse mentoring with senior members of the workforce (Alcorn, 2016). Older people are given guidance in the effective use of social media (PwC, 2013) and encouraged to incorporate online ‘productivity tools’ into their work lives (Lyall Grant, 2016). This impetus to increase online collaboration and interaction pushes users to place trust in new technologies. Those not instinctively technological are persuaded to use apps which may be accessing a large volume of personal data. An average user may not recognise an application from a disreputable source or sense suspicious activity. Younger people and avid users may be so enthralled by the connected community that security aspects of new

technological trends are not considered (Otey, 2013). Millennials raised with continuous access to social media, and a dependence on applications will most likely continue their relationship with technology when they reach corporate board level. Advantageous for the company business model yet creating further complications for maintaining security. (**RQ1 actual/perceived risks**).

3.9.6 Shadow Systems: Shadow IT

Within the corporate environment, computers, software, and associated technologies are typically the domain of the Information Technology (IT) department. IT services design, operate and support the IT infrastructure, including the communication network, storage and management of data and system security. Support service teams also aid and assist end-users of digital resources, ordinarily via a 'helpdesk' where users can access online, phone or face-to-face support. The culture of BYOD and widespread use of privately owned devices for work purposes has forced IT departments to develop security mechanisms to secure mobile working and access to corporate data. In essence, if IT services know which devices connect to the network and can retain control over software and apps used by personnel, then security can be maintained. Shadow IT is defined as "the phenomenon of user-driven fulfilment of requirement" (Györy et al., 2012, p. 1) and consists of software and applications installed by employees without approval from IT managers. Examples include productivity and communication applications, internet browsers and content management tools (Silic and Back, 2014, p. 278). Users have introduced (without consent) so many technologies into the workplace, that IT managers fear they have lost control of security (Carter, 2015; Chapman, 2015; Froehlich, 2015).

Shadow systems are informal and therefore not obvious (Behrens, 2009) and may introduce unexpected risks to organisational security, with “potentially serious impact” (Silic and Back, 2014, p. 274). Shadow IT may be considered as noncompliance with security protocols and classified as an insider threat (György et al., 2012). (**RQ1 actual/perceived risks** and **RQ2 average usage/impact**).

Contemporary employees require faster, more responsive technologies to increase productivity, and are finding their own solutions when corporate systems are lacking. This increases the risk that those with less technical skill may be installing compromised software (Silic and Back, 2014, p. 278 (**RQ1 actual/perceived risks** and **RQ2 average usage/impact**). Besnard and Arief (2004, p. 253) discuss “trade-offs” where computer users overlook rules to gain benefits of usability, despite the consequence of lapses in cybersecurity. Furthermore, actions which give immediate benefits to the user are often given priority to the detriment of long-term security (**RQ1 actual/perceived risks** and **RQ2 average usage/impact).** To circumvent imposed controls, employees with enhanced technological skill are using portable apps which require no administrator rights and show no visible modification (Silic and Back, 2014, p. 278). Many productivity tools, games, media players, editing and chat/messenger software (Yamada, 2019) can be stored on a flash drive and accessed on any computer operated by the user. Sharing external drives between systems can spread malware or other malicious content (Portable Apps, 2016). Safeguarding digital systems by restricting access to only those with authorisation can prevent users from making unauthorised configurations but may instil distrust between IT services and business personnel. Fürstenau, Rothe, and Sander (2020)

recommend that a relationship of trust, or at minimum, mutual respect will possibly limit the amount of shadow systems developing in an organisation.

Interestingly, Silic and Back (2014, p. 279) suggest that employees “naively” believe that they are not committing an actionable offence by the installation of shadow IT applications. This is because workers download freely available open-source software, rather than licenced products which have been obtained illegally (**RQ1 actual/perceived risks** and **RQ2 average usage/impact**). Digital natives and millennials are familiar with complex technology and may be contributing to shadow systems. The aspiration for “the latest and shiniest” technologies (Kapuria, 2008, part 8), entails the installation of new apps and shortcuts to circumvent old programs (Otey, 2013, p. 205). Furthermore, millennials with advanced skills are likely to search for and locate tools to evade restrictions placed on content they wish to access, for example, social media sites (Humphries, 2015) (**RQ1 actual/perceived risks** and **RQ2 average usage/impact**).

In contrast to the security risk, Behrens (2009) proposes that shadow systems are more efficient than formal systems. Formal IT may be too outdated for users’ accustomed to intelligent and responsive software, and shadow IT may utilise better facilities. An effective shadow system which attracts attention of corporate stakeholders may provide opportunity for the system to enter business use and obtain governance of the IT department (Fürstenau, Rothe, and Sandner, 2020). Besnard and Arief (2004) recommend that those responsible for designing and managing IT infrastructures should analyse the areas where users are likely to

take shortcuts. Subsequently, security policies and protocols allowing for “intuitive notion of usability” can be initiated (Besnard and Arief, 2004, p. 256). A shadow system might be a model for a more efficient IT infrastructure and enhanced systems can be created by observing where users have inserted modifications and improvements.

3.10 Summary of 3.9 in Relation to Research Questions One and Two

In relation to **RQ1 (actual/perceived risks)** a real threat to organisations may arise from decisions made by third parties who will never operate corporate technology. Frequent changes may confuse operators, particularly when familiar systems no longer function as expected. Employees are expected to work with complex software as part of a daily routine, and regardless of a users’ competency, they are unlikely to fully understand the technologies they work with. As an example, applications may contain non-essential features which should be disabled. Alternatively, employees with little interest or understanding of technology may be overwhelmed by the systems or software they are expected to use. Personnel may be given responsibility for system support which should be managed by administrators, thus expanding the margin for error.

Employees may take part in training sessions which do not adequately explain the risks that technology entails. An organisation might expect that training has explained the use of corporate systems, but online risks may not be understood. If users are unfamiliar with the myriad internet threats and do not relate to them in a personal context, a lack of cyber awareness may contribute to unsafe behaviours during internet activity or while interacting with cloud services. Thus, a

risk of succumbing to online harms may be consistently present in the workplace. In relation to **RQ2** (**average usage/impact**) and how users make use of privately owned devices, meagre cyber awareness by an imprudent owner may leave vulnerabilities on a portable device. The user may download or share content, free apps and participate in inappropriate internet use. Similar internet activity on multiple devices may exacerbate risk of a compromised network if the owner brings them all to the workplace. Organisations can restrict access to corporate data, yet employees may still access the network for messaging services, emails or calendars and diaries. A device not connected to the network might still be a threat, as malware can spread via sharing of files including work documents or personal media files. As an additional risk, undisclosed devices in a bag or pocket can share and be susceptible to malicious code if the Bluetooth system is activated.

A workforce consisting of a diverse range of ages will present differing levels of technological skill. Although accidental or inadvertent harms via incompetent users is still possible, an actual risk is that the workforce is too technologically competent. Highly skilled personnel may find hierarchy and formal systems too restrictive and use the internet to find their own solutions. As new technologies appear and are adopted by users in their personal space, they will no doubt be introduced illicitly into the corporate network. Technically proficient employees may then encourage those with less competency to engage further with online tools and platforms. This may then present new opportunities for accidental or inadvertent harms as less skilled users install compromised applications or are faced with more complex software they do not understand. This has relevance to **RQ1 actual/perceived risks and RQ2 average usage/impact** as users create an

actual risk through shadow systems, and the personal use of mobile devices may contribute to this.

3.11 The Internet of Things (IoT)

Research Question **RQ3** is concerned with evaluating the presence of Internet of Things (IoT) devices in the workplace and the unexplored potential for risk. This next section introduces IoT and provides an explanation of smart technology and the intended purpose of IoT systems. An evaluation of wearable devices leads to an examination of the potential cyber risks created by unsecured applications, infrastructure and operating systems present in IoT units. The section concludes with a discussion about shadow IoT systems in the workplace and the potential impact on corporate security.

3.11.1 Smart Technology

'Smart' or 'intelligent' ubiquitous technologies are creating a potential new risk to the business sector. Alpaydin (2016) defines ubiquitous computing as the use of computers without the knowledge of computers being used. This can be placed in context by recognising that many digital systems are used for a variety of purposes, ostensibly all the time, without the user identifying them as computers. Most contemporary lifestyle devices are either computers or contain a computerised system. Televisions, cars, cameras, microwave ovens, digital alarm clocks (Popyack, 2008) and many other commonplace units all contain computerised systems.

Smart technology is established in manufacturing, retail, automotive, healthcare, town planning and building management (Weinberg et al., 2015). Smart units gather data through embedded sensors and analyse and share information to make real-time decisions (Carrino et al., 2016). Devices are connected to the internet and communicate via machine-to-machine communication systems (Botelho, 2013). Thus, the network of connected sensors, devices, and objects (Perera, Liu, and Jayawardena, 2015) is known as the Internet of Things (IoT), clarified by Ashton (2019) as "computers gathering information by themselves". Manufacturers strive to develop services to enhance safety and wellbeing for users (Dohr et al., 2010) and generate more free time as machines take on tedious tasks (Moser, Bruppacher and Mosle, 2010). The IoT is expected to change the online 'virtual' space to a dynamic network created by connected objects present in the physical world (Dohr et al., 2010).

It is important to differentiate between devices recognised as IoT and others which are web-enabled (Setterstrom, Pearson and Orwig, 2013). Laptops and smartphones may connect to the internet but are not considered to be IoT devices. Credited with first using the name 'Internet of Things', Ashton (2010, para. 5) stated the necessity to "empower" computers, enabling them to "see, hear, and smell the world for themselves". More recently Ashton (2019) describes IoT as a 'sensitivity device' for example, an internet connected GPS (Global Positioning System) device or thermometer collecting data to be aggregated, compared and shared (Ashton, 2019). For a device to be considered 'smart', it must sense changes in environment, condition, motion, or circumstances, and have capacity for autonomous reaction. Smart devices 'learn' by recognising

patterns in data and support industry by automating tasks and removing the necessity for human control and intervention (Plummer et al., 2015). These technologies offer “enormous benefits in performance, efficiency, operating costs and endurance” (Worden, Bullough and Haywood, 2003, p. 1). To illustrate, intelligent systems in a smart building will use sensors embedded in the environment to track location and movement of occupants, analyse use of space and automatically adjust ventilation and lighting (Roth, 2016). Smart cities and towns use data collected from connected devices to meet specific needs, for example, “dynamic streetlight management” (Carrino et al., 2016).

3.11.2 Consumer IoT

In theory, any object can be connected to the internet, made possible by the reduction in the cost of sensors and an increase in capability for data processing and connectivity (Britton, 2016). 5G mobile connectivity is anticipated to facilitate IoT expansion and over thirty billion devices are predicted to be online by the end of 2020 (Statista, 2020c). The first generation of smart devices and systems aimed specifically at consumers included home security devices with motion or temperature-controlled cameras, environmental heat and lighting controls, and fridges which monitor contents (Storey, 2014, p.9). Appliances included coffee percolators, robotic vacuum cleaners, pet monitoring cameras and baby monitors. A contemporary innovation is the voice activated ‘virtual assistant’ (VA) such as Alexa, Siri, or Cortana. Users can now use a VA as a ‘hub’ to operate a multitude of home devices, such as environmental controls and appliances. In place of command-and-control applications downloaded to a smartphone or tablet (Hewlett Packard, 2015, p. 3) each separate unit can be added to the virtual assistant.

Devices are then operated via the VA app (Nield, 2019) or activated by voice commands (Giannoulis, Potamianos and Maragos, 2019; Lynch, 2020). If the user chooses to bestow device control to a virtual assistant, this may result in potential security issues since the app for each individual unit is not made redundant (Nield, 2019). Unfrequented apps may then be hidden amongst the content on a user's smartphone. If a user does not visit the app, they may not be aware of any security notifications, unless the virtual assistant takes responsibility for managing updates **(RQ3 IoT unexplored risk).**

Manufacturers are competing to embed IoT technology in more devices and voice activation will be the next evolution for the consumer market (White, 2019). For some users, purchase of a virtual assistant will initiate further investment in smart technologies (Ammari et al., 2019, part 4.4). Consumer devices now include novelty units such as showers, bathroom mirrors and toilets (Vincent, 2019) wine bottles, dental floss and underwear (Coward, 2018). Nonetheless, a low budget device may have poorly configured accompanying software security (Junior et al., 2019; Wang et al., 2019) **(RQ3 IoT unexplored risk).** If the virtual assistant is used as a control hub, the user may not be aware of any potential risk if all access takes place using the VA instead of the app **(RQ3 IoT unexplored risk).**

Alongside industrial IoT in business premises, consumer IoT may be establishing a presence in the corporate workspace. IoT might be represented virtually by applications on smartphones or as a physical entity if an appliance has value as an addition to the working environment. To illustrate virtual representation in context, domestic appliances such as a vacuum cleaner or washing machine may

be operated remotely by app from a user's workplace. If the app is downloaded to a smartphone connected to the corporate network, the IoT unit is virtually present in the workplace. Physically present IoT may be an appliance which enhances the office facilities, such as a kettle or coffee percolator which can be activated by smartphone from a meeting or conference. Devices not typically recognised as IOT units may additionally be present in the corporate environment. Smart plugs are a cost-effective method to allow standard electric powered devices to be controlled from a phone using a Wi-Fi network (BT, 2018; Jones, 2020). A printer, fan or lamp may be controlled by employees enjoying the facilities provided by their 'connected' office without recognising they are using an IoT unit. Average users might not comprehend that the plug is susceptible to vulnerabilities (Ling et al., 2017) and could be an access point into a corporation (DeNisco-Rayome, 2018) or used to compromise a network (Zorz, 2018) **(RQ3 IoT unexplored risk).**

3.11.3 Wearable Devices

Smart and intelligent wearables are small "body-worn" devices, developed for the consumer market, popular due to compactness and wearability (Yoon, Park, and Lee, 2016) and may be another example of physical IoT in the workplace. There have been many attempts to introduce wearable technology to consumers, for example, the Google Glass optical computer system (Swider, 2016) and several generations of web-enabled watches. These wearables were not embraced with the same enthusiasm as less obtrusive health monitors (Ernest Young, 2015, p. 4) and failure to meet expectation resulted in limited acceptance (Coorevits and Coenen, 2016). Contemporary smartwatches incorporate streamlined, aesthetic design, health and fitness monitoring, and include NFC payment facility. For the

consumer, a desirable feature is that the device operating system no longer requires support from a smartphone (Loterina, 2016). Medical devices to monitor health conditions and dispense medicines (Pak and Park, 2012; Park and Pak, 2012) are now so unobtrusive they can be worn as gloves, spectacles, an earpiece, or shoe (Zheng et al., 2014). Consequently, Liu and Sun (2016, p. 45) describe intelligent wearables and "people-centric IoT" as a "gateway" between humans and other IoT devices and applications. At present, a smartphone is used to connect the user and device (Perera, Liu, and Jayawardena, 2015).

A primary feature of 'smart' technology is pattern recognition and the capacity to 'learn' from collected data, thus augmenting performance (Plummer et al., 2015). A very simple example relating to consumer IoT is how an individual may evaluate data collated by fitness monitoring and increase healthy activity accordingly. The longer a fitness tracker is worn, the more data is accumulated to determine the habits of the user. If the individual makes consistent adjustments recommended by the analysed data, augmentation of performance can be increased. Industry experts originally predicted that five hundred and eighty million (580,000,000) internet-connected wearable devices would be operational by 2017 (Plummer et al., 2015) and consumers would adopt IoT as mainstream when fitness trackers gained capacity to conduct contactless payments (Mintel Group Ltd, 2016b, p. 34). Despite this, acceptance of consumer and home IoT has not yet reached the level initially forecast (Daly, 2016; IoT for All, 2020; Landman, 2019; The Internet Society, 2019; Titcomb, 2016), although wearable fitness devices have achieved greater success in the UK market (Mintel Group Ltd, 2016a). Contemporary analysis forecasts that over one billion wearable devices will be in operation by

2022 (Liu, 2020) and eyewear (Darafsheh, 2019), and earwear (Langley, 2020) will continue to drive the technology forward. Employees may eventually be required to wear fitness devices as a condition of employment (Plummer et al., 2015). Already, some organisations are asking employees to voluntarily wear fitness trackers to monitor physical activity and sleep patterns (Gilligan, 2017).

Smart jewellery is a contemporary trend in wearable devices, aimed at the discerning consumer who finds plastic and silicon smartwatches and wristbands unattractive but would like the facilities of fitness tracking and notifications from apps. Rings, bracelets, and necklaces created from precious metals and gems, incorporate tracking sensors and operating systems and are indistinguishable from conventional pieces (Charara, 2017; Gokey, 2016). Smart clothing originally appeared as an experiment by fashion designers who used intelligent fabrics as a spectacle for the catwalk (Kobie, 2015). Garments made from smart textiles enable a “dynamic interface” between the human body and the environment and the generated data influences behaviour of the garment and of the wearer (Frances et al., 2017, p. 9). The concept of ‘soft wearables’ (ibid., 2017) has expanded to include thousands of connected garments and footwear with each item controlled via an app on a mobile device. The intention is for interactive, personalised apparel for the consumer, and the potential for industry to secure access to real-time analytics (Arthur, 2016). Smart textiles also appear in healthcare, where sensors to monitor medical conditions and vital signs can be embedded in fabric employed for personal medical devices (Zheng et al., 2014).

3.11.4 IoT Security Risks

Even if IoT acceptance has not achieved industry expectation, technology enthusiasts may be purchasing new gadgets, appliances and systems aimed at the home market, or trying out wearables, textiles and unobtrusive personal medical devices. Sales of smart devices increase during seasons where gifts are exchanged (Thurrott, 2019) and the quantity of IoT entering the corporate environment increases after a significant holiday for example Christmas (Open DNS, 2015). Hence, IoT may already be present in the workspace, due to wearable devices and home gadgets received as gifts or purchased at discounted price during a retailers' sales period. The security aspect of wearable IoT is a concern, for fitness trackers and watches can be concealed beneath clothing and garments and jewellery are indistinguishable from conventional pieces. Furthermore, employees may not wish to disclose the use of medical devices. Hence, security managers and risk assessors may not realise the scale of IoT present in the workplace and any possible threat to the IT infrastructure **(RQ3 IoT unexplored risk).**

Cybersecurity can be complex, and Internet of Things devices maintain multiple facets which must be considered. The IoT "eco-system" operates on three separate levels: the device, supporting applications, and cloud infrastructure (Spiezle, 2016, p. 3). Each layer is susceptible to vulnerabilities created through flaws in code or logic and security should be incorporated at the design stage (Miorandi et al, 2012). Manufacturers are hastening to bring new devices to market without full consideration of the threat landscape and are failing to employ sufficient security protocols (Britton, 2016). Cost or time limitations (Spiezle,

2016; Verizon, 2015, p. 63) may be a contributing factor, or manufacturers may lack expertise to implement “security safeguards, privacy controls or lifecycle support plans” (Spiezle, 2016, p. 2). A manufacturer may not have facility to conduct due diligence on all suppliers of components, hence lack of provenance regarding supply chain providers may affect robust security (Carr, 2019). Devices produced by competing brands will employ varying levels of encryption and alternate methods of connectivity. Thus, a mélange of systems will evolve which may prove difficult to maintain and upgrade (Sarma, 2015). Miniature sensors and small devices compound the issue, for they may not be equipped with adequate processing power or sufficient memory to implement the necessary layers of security (Bertino and Islam, 2017; The Next Wave, 2016). **(RQ3 IoT unexplored risk).**

Early IoT models may be redesigned or relaunched by manufacturers who will no longer offer software support to the original version, leaving unpatched or outdated devices attached to a network (Hoffman, 2016) **(RQ3 IoT unexplored risk).** Spiezle (2016) recognises that devices may be transferred to new premises or change ownership and advises that support services should continue beyond the expiration of a device warranty **(RQ3 IoT unexplored risk).** Many consumer devices are sold with insufficient security measures (Scott, 2016) and models which do include pre-installed protective mechanisms depend upon users to remain aware of security issues. Owners must take responsibility for maintenance, and obtain available patches or updates (Spiezle, 2016; The Next Wave, 2016). Nevertheless, expectation that owners will be proactive towards security may create further issues. If the user considers their device to be a

fashionable toy, they may not endeavour to keep abreast of security concerns **(RQ3 IoT unexplored risk)**. Consumers should also be aware that expensive IoT models are more likely to have inbuilt security and significantly cheaper models are (often) unprotected (Krotoski, 2017). There is an identifiable need for streamlined updating mechanisms, for incidents can happen when users fail to respond to alerts from the manufacturer (The Next Wave, 2016) **(RQ3 IoT unexplored risk).**

Liu and Sun (2016) suggest that wearable IoT devices may be a potential initial attack vector, due to their position as gateways between devices and applications. The authors caution that lightweight operating systems common in small devices will share the same vulnerabilities. An attack against a wearable device could allow access to other systems, enabling sharing of malicious code or compromise of personal data **(RQ3 IoT unexplored risk).** As devices collect sensitive data and are always connected to the internet, there is increased opportunity for violation (Britton, 2016; Siboni et al., 2016)**.** Proof of Concept (PoC) exploratory attacks have been observed against IoT devices, testing for vulnerabilities and security flaws (Scott, 2016; Verizon, 2015). These ventures are reminiscent of the telephone 'phreakers' who experimented with early communication networks to understand the complexities of the telephone system. Donovan (2016) describes 'phreaking' as a practice of discovery and experimentation and PoC attacks originally adhered to this model without intending to generate profit (Barcena and Wueest, 2015). Nonetheless, phreakers did eventually learn to exploit vulnerabilities and steal free phone calls (Lapsley, 2013; Mitnick, 2001) and in

common with other computerised systems, smart technology is likely to attract criminal interest.

Corman (2016, quoted by Hewlett Packard Enterprises, 2016) warns that any device using software is ‘hackable’ and if internet connected, is ‘exposed’. Security researchers have observed “a large number of application vulnerabilities developed by manufacturers”, introduced by using “simple” and “unsafe code” to hasten product development (Yu et al., 2020, p. 5). IoT units are connected to the internet and are therefore vulnerable to threats including “malicious code hacking attacks” (Vermesan and Friess, 2014, p. 91). Such attacks may utilise IoT specific malware (Costin and Zaddach, 2018) and polymorphic code (Darabian et al., 2020) engineered to defeat traditional detection methods (see 3.3.2). Deschamps-Sonsino (2017) discusses how an email address used by to register a smart refrigerator for warranty purposes was hacked and used to send spam email. Symantec (2016, p. 16) declare that if a device can be hacked, then “it probably will be”.

In 2016, a vast network of infected, computerised machines was instrumental in a disruptive Distributed Denial of Service (DDoS) attack. The significant difference between this episode and previous botnet attacks was that the units involved were Internet of Things devices. Unsecured routers, digital video recorders, webcams, security cameras and baby monitors were all active in the attack (Chan, 2017; Solomon and Fox-Brewster, 2016). The Mirai malware responsible for the compromised units continually scans the internet seeking vulnerable connected machines (Mansfield-Devine, 2016) and uses a list of sixty-two default usernames

and passwords to gain access (Bertino and Islam, 2017). Hence, the necessity for proactive security from user/owners becomes apparent as without secure protective measures, non-traditional devices including printers, fridges, thermostats, or toasters may become part of a compromised network (Symantec, 2016). Despite the high-profile attack, vulnerable IoT including webcams, routers, and wireless access points, are still being identified and attackers may continue to access a system, propagate malware, and perform DDoS attacks (Numaan, Hilt, and Hellberg, 2017). **(RQ3 IoT unexplored risk).**

IoT units are appearing in highly regulated industries, but there is a significant gap between mitigating controls and the number of devices in use (Open DNS, 2015) **(RQ IoT unexplored risk3).** Within the enterprise environment, Moyle (2016, para. 5) recommends security measures take place on a "case by case, device by device basis" and security managers should have knowledge of the IoT present in the workplace. If physical devices have been purchased using a departmental budget, an audit trail of purchase orders and receipts should alert security managers to their presence; but employee IoT may be harder to trace. Wrist worn devices are unobtrusive and therefore undetectable and insulin pumps or pacemakers (Corman, 2013), may be obscured by clothes, or undisclosed by personnel. Unless stakeholders are aware of the existence of 'soft' wearables, they may not expect to find connected socks or garments in corporate workspace. The volume of devices present on company premises may be unknown and it is not inconceivable that attackers might hack an organisation via the office coffee maker or wearable fitness tracker (Corman, 2016, quoted by Hewlett Packard Enterprises, 2016) (**RQ3 IoT unexplored risk).**

Factory issued default passwords are a recognised vulnerability that invite attention from attackers. IoT devices using default passwords have been exploited to gain entry to an organisation (Anderson, 2019; Microsoft, 2019) or infected with malware which “co-opts them into botnet armies” (F-secure, 2019, p. 8) (**RQ3 IoT unexplored risk).** As a response, the UK will introduce legislation to ensure future consumer IoT is “secure by design” (Minister for Digital and Broadband, 2020, p. 8) with robust mechanisms implemented from the planning stage. This is intended to combat the risk enabled by factory issued passwords and additionally the failure of consumers to pursue security information. Buyers are not proactive at security research as they typically believe that devices have inbuilt protective mechanisms when they go on sale (Harris Interactive, 2019, p. 3; Minister for Digital and Broadband, 2020, p. 6) (**RQ3 IoT unexplored risk).** The new legislation will include the necessity for unique passwords, alongside requirement that consumers are informed of the duration of support a device can expect to receive (Warman, 2020).

The Internet of Things has created challenges to traditional risk management procedures, as conventional practice expects that assets and data are owned and possessed by an organisation (Ernst and Young, 2015). IoT systems transmit data to external servers and the infrastructure is predominantly cloud-based, hence data is no longer (necessarily) held securely within company boundaries. As an additional risk, command-and-control applications to supervise ‘smart’ units may be installed on employee-owned mobile devices. IoT apps may have no secure connection to the cloud infrastructure (Barcena and Wueest, 2015) hence,

mobile devices entering the workspace might introduce a previously unconsidered threat to the network (**RQ3 IoT unexplored risk**). The unpredictable nature of converging technologies may create new opportunities for criminal behaviour and misuse in ways not anticipated by manufacturers (Morris, 2004). Mixing infant and legacy technologies; for example, artificial intelligence, machine learning, cloud services and the internet, may cause a high impact 'Black Swan' event (Taleb, 2007). An extremely rare, chaotic event, unthinkable on occurrence (Griffin and Stitt, 2009) and unpredictable at the time, a Black Swan can only be predicted retrospectively (Taleb, 2009, quoted in Mckinsey Quarterly, 2009) **(RQ3 IoT unexplored risk).** In the context of assessing risk for IoT technologies, it is apparent that a disruptive technology, combining elements of old and new systems, hastily pushed to market is prime for an unexpected event. This is particularly relevant since smart objects create ad-hoc connections following unpredictable patterns (Miorandi et al, 2012).

The Internet of Things may be the precursor to an Internet of Everything where "Human beings, pets, farm animals, and computers, books, cars, household appliances and food" will all be connected to an online network (Tweneboah-Koduah, Skouby and Tadayoni, 2017, p. 172). Thus, consideration of Black Swan logic whilst conducting technological risk assessments may have merit. The logic does not enable foresight of where, when, how or what an impact will be but recognises that the future is unpredictable, and that chance is always unknown (Stojanovic, 2011). This again raises the question of guardianship, as seen in the concept of cyber-specific RAT. At present, responsibility lies with the user and expectation is that networks will be protected by strong passwords and vigilance

towards system updates. The security risk consistent with this model is that users often neglect applying security patches to computers and mobile devices, therefore updating IoT units may not take place. (Palmer, 2017b) (**RQ3 IoT unexplored risk).**

The issue of user as assumed guardian is topical, as some homes already contain many objects and systems with 'smart' connectivity, and new 'must have' gadgets are introduced regularly. The avid user is expected to manage substantial security; thus, neglected guardianship may become an ongoing concern. Furthermore, in accordance with many other technologies, some IoT devices have been upgraded to new generations, incorporating enhanced features. The user who purchases a new device to update an older model may no longer take responsibility for the previous unit, thus an absent guardian may facilitate victimisation. A further consideration concerns wearable devices and the "large attrition rate" of consumers who no longer wear fitness trackers (Coorevits and Coenen, 2016, p. 1). The authors demonstrated that users forsake their wearables for a variety of reasons and do not always delete the command-and-control application. From a security perspective, an abandoned wearable may not receive any further security updates. If the accompanying application is no longer used, it too may not receive any relevant security patches thus rendering the device it sits upon vulnerable to exploit. (**RQ3 IoT unexplored risk**).

3.11.5 Shadow Systems: Shadow Internet of Things

The expansion of internet connected devices is exacerbating the predicament of security managers who would appear to have lost authorisation over the information technology appearing in the workplace (Russell, 2016). When

decision-makers purchase ‘smart’ equipment for internal departments without discussion and consent from IT managers (Chapman, 2015) a ‘shadow’ Internet of Things can evolve. Hence, Russell (2016, p. 18) proposes that current IT risk assessments are updated and evaluated against each department on an individual basis. The author advocates a bespoke assessment rather than ‘one size fits all’ and the end-users of technologies should be a factor included in the risk evaluation. Furthermore, as a consequence of consumer IoT reaching a wider market and novel devices appealing to new users, risk managers should consider that a IoT shadow system may evolve when employees carry and wear unauthorised items into the workplace. Millennials might be early adopters due to their enthusiasm for new technologies (Otey, 2013) or healthcare providers may issue connected monitoring devices to patients. Once health and fitness trackers gain NFC payment functionality, they may find a mass market. Phones or tablets acting as the interface for IoT devices and loaded with control applications might contribute to an expanding shadow IoT without IT professionals realising it exists (**RQ3 IoT unexplored risk).**

Many organisations have legacy IT infrastructure in place which cannot easily be replaced without a full refurbishment of the corporate network. Thus, new technologies are added ad hoc to an existing foundation, creating a ‘patchwork’ of systems (Sarma, 2015) (**RQ3 IoT unexplored risk**). Security research identifies that some IoT devices are connecting to old infrastructure and encountering outdated security certificates, (Hay, 2015; OpenDNS, 2015). Plummer et al. (2015, para. 8) forewarn that when smart devices reach a level of intelligence allowing them to transcend simple autonomous, predictive behaviours, then

“unexpected and potentially unwanted results” can occur. This concurs with Black Swan logic and the concept that unforeseen factors should be considered. Security managers may be advised to assume that shadow systems are already in place and apply risk mitigation accordingly. (**RQ3 IoT unexplored risk**).

3.12 Summary of 3.11 in Relation to Research Question Three

Research Question Three is concerned with consumer IoT in the workplace and aims to theorise unexplored risk. Enterprise security managers have adjusted protocols in the sectors where industrial IoT is already well established, but the literature makes no reference to consumer units and possible impact of employee IoT. Security managers should recognise employee IoT so that risk assessments can include personal devices and applications. This has relevance to **RQ3 IoT unexplored risk**, as employee devices or wearables may be consciously hidden or accidentally concealed. Employee IoT may also have accompanying command-and-control apps installed on a privately-owned portable device. Alongside minimal IoT device security, applications may also be compromised through poor programming language, creating more security risk to the enterprise environment. IoT devices and sensors may be small, with limited processing power and inadequate capacity to run security systems. Devices with vulnerabilities in common may share compromised code. This may subsequently infect a corporate network, potentially via an unsecured app on a smartphone.

A device no longer updated or supported by the manufacturer is a security risk to a network, therefore users are responsible for remaining informed about potential risks. Despite the drive to push IoT devices to market, there has been little

indication from manufacturers regarding the need for users to assist devices to remain secure. Devices depend on users to proactively manage security, yet a user may be unaware of the risk, unfamiliar with how to maintain security, or simply just forget. Trend forecasters may be accurate when they predict that NFC payment systems will contribute to a shift in consumer attitude. Wearables may then become mainstream, paving the way for widespread incorporation of home systems and appliances as manufacturers continue bringing innovative devices to market. Consumer IoT has not yet reached maturity, and all potential threats may not be apparent. Nonetheless, an unpredictable event instigated by convergence of new and legacy technologies is plausible. Once smart devices achieve mainstream acceptance, many owners may not consider the security aspects since users typically retain an unassailable sense of trust in technology. As smart technology develops and incorporates novel features appealing to a wider market, organisations with no current shadow IoT will likely find it manifesting in the future. Risk assessment of IoT in the workplace should be considered as a priority.

3.13 Analysis of the Literature Review

Academic literature pertaining to computers and the internet tends to be technological in nature, offering new solutions or frameworks for security and code development and is aimed at academics or IT professionals with understanding of computer science or IT networks. The language of computing is technical in nature and obfuscating discussion can exclude interested readers. This is a limitation, for literature is intended to educate and inform and alienating the reader fails to impart knowledge. It is therefore intended to present findings from this study in a format to be accessed and understood by those without specialist IT

expertise. When discussing the human element of technology, the literature addresses insider threat (AgrafIoTis et al., 2015; Furnell and Clarke, 2009; Saxena et al., 2020; Ring, 2015; Warkentin and Willison, 2009), necessity for robust cyber security training (Colwill, 2009; Salim and Madnick, 2014; Silic and Back, 2014) and assessment of perceived risk through use of IT systems or the internet (Byrne et al.,2016; Coles and Hodgkinson, 2008; Sjöberg and Fromm, 2001;Tsai et al., 2016). Literature addressing personal technology use in both personal and corporate space appears to be absent, and research evaluating use of personal Internet of Things devices as a risk factor is additionally lacking.

A theme identified in the literature is how IT professionals, rather than average users, are recruited as samples for qualitative studies regarding technology use (György et al., 2012; Kraemer, Carayon and Clem, 2009; OpenDNS, 2015; Silic and Back, 2014). In addition, pre-existing surveys completed by IT practitioners have been used for analytic purposes (György et al., 2012; Silic and Back, 2014). On occasions when a sample was recruited from company personnel, respondents came from a single organisation (Silic and Back, 2016), were randomly selected from various sectors (Coles and Hodgkinson, 2008) or surveyed on a specific aspect of technology, for example, social media management (Wilcox and Bhattacharya (2020) or multiple social media use in the workplace (Forsgren and Byström, 2018). Lack of consultation with end-users is recognised as a limiting factor (Silic and Back, 2014). Therefore, this study will survey employees to analyse technological behaviours and attitudes and the sample will be recruited from a sector reliant on computerised systems. The additional gaps identified in this review will be addressed by an emphasis on the

actual use of technology, regardless of any perceived risk of use and aim to modify existing literature by enhancing knowledge of insider threat.

The literature indicates that the Internet of Things is a continually evolving technology on the verge of mainstream acceptance. Risk and security managers may have prepared for industrial IoT in the workplace, but thus far, the market for consumer IoT lacks complete engagement from customers. Hence, managers may lack knowledge of the volume of IoT on company premises. This research may confirm that employees have not yet embraced IoT technology and security managers still have opportunity to configure protective solutions. Alternatively, the findings may reveal that Shadow IoT is endemic throughout the corporate environment and security protocols may need urgent revision.

3.14 Conclusion to the Literature Review

Chapter Three began by documenting the financial sector response to threat of cybercrime to establish the rationale for considering employee (mis)use of personal technology as a contributor to cyberattack against corporate systems (3.2). The current model of insider threat accepts potential for harm from disgruntled or vengeful workers and threat to an organisation from lack of competence or abuse of insider knowledge (3.2.1). In parallel with the financial sector, employee use of personal technology is not (apparently) considered a threat to corporate networks. Evaluating academic and security literature through the theoretical lens of cyber-RAT identifies myriad opportunity for convergence at all levels of digital infrastructure. Ranging from unavoidable software flaws creating vulnerabilities for exploitation (3.3.2) relevant to **RQ1 actual/perceived**

risk; RQ2 average usage/impact and **RQ3 IoT unexplored risk,** to motivated offenders trading in automated crime services to deliver multiple attacks to affect internet users (3.3.1) (**RQ1 actual/perceived risk; RQ2 average usage/impact** and **RQ3 IoT unexplored risk)** and deliberate targeting of mobile operating systems (3.7.2) applicable to **RQ2 average usage/impact**, the literature establishes technology as a vast landscape of potential threat**.** Suitable target may be instigated by routine access to cyberspace, and cyber-RAT finds opportunity for convergence in social media in the form of social engineering (3.4.1) phishing and targeted assaults (3.4.2) applicable to **RQ1 actual/perceived risk** and **RQ2 average usage/impact**, and malware attack (3.4.3) relevant to any internet user (**RQ1 actual/perceived risk)** or those using mobile devices for online access (**RQ2 average usage/impact)**. Other opportunities for convergence arise with the use of 'instruments' extending the reach of offenders, engineered for stealth and detection avoidance (3.3.2) and pertinent to **RQ1 actual/perceived risk**; **RQ2 average usage/impact** and **RQ3 IoT unexplored risk**. In respect to emerging technology and **RQ3 IoT unexplored risk,** tiny operating systems with limited processing capacity, hurriedly manufactured software, a haste to reach market and limited capability for security may position device and consequently a network as suitable target. Potential for convergence with a specifically designed IoT instrument (3.11.4) is a risk faced by smart technologies.

A new perspective of the employee as a risk to corporate assets is proposed (3.9), to consider evolution of technology, a society of networked users, shadow systems and possible lack of knowledge of the complexity of internet harms and

how to secure against them. Personal internet activity may have unexpected implications for a corporation and a user's attitude to internet safety may exacerbate the impact**.** Thus, the employee and device use are relevant to **RQ1 actual/perceived risk**; **RQ2 average usage/impact** and **RQ3 IoT unexplored risk**. The human element of corporate cyber security may benefit from reappraisal, to reflect contemporary attitudes and behaviours and redefine the parameters of insider threat.

The next chapter (Chapter Four, 'The Corporate World') documents the first stage of the digital investigation to find a purposive sample of average-user financial services employees. The cyber-Rat framework will be seen to evaluate routine digital activity in the context of motivated offender, suitable target and absent guardianship. The chapter begins by offering justification for the unorthodox presentation of three methodology chapters, representing a single methodology across three different groups, before introducing the research methods in 4.4.

Chapter Four: The Corporate World (Methodology One)

4.1 Introduction to the Methodology Chapters

This project is grounded in technology. The research problem was inspired by a real-world technology-driven issue (see 4.2) and consequently required a digital-led research strategy (see 4.2) drawing on the researcher's internet-based professional experience (see 4.3.4). As an (unanticipated) consequence of utilising online research methods, the written work deviates from the recognised format of a doctoral thesis and offers three standalone methodology chapters. Although each chapter is unique in the methods recorded, they each represent a single stage on the chronological journey taken to recruit a sample ideally suited to answering the research questions (see 1.2). A chapter could not be omitted without leaving a gap in the overall methodology, therefore, all three are included to demonstrate the challenges and possibilities of digital investigation and act as a 'roadmap' for replication and improvement by other researchers. The reader should note that the open-source internet investigation described in Chapter Four, 'The Corporate World' and Chapter Five, 'Executive Risk' preceded the introduction of the General Data Protection Regulation (GDPR) and the Data Protection Act (2018) and was conducted following the principles of the Data Protection Act (1998). The impact to the project caused by the introduction of the GDPR, including a new application for ethical approval and restructuring of the electronic survey is described in Appendix D.

To appreciate why the thesis offers three methodologies, it is first necessary to recognise how the research methods evolved. Section 4.2 begins by defining the

nature of the phenomenon in question and presents the stimulus for the investigation, followed by an overview of the research strategy to determine viability of the internet as an intelligence tool. Section 4.3 establishes positionality and reflects on philosophical frameworks, ethics and values as instigator and inhibitor of successful digital research. Section 4.4 summarises the research strategy in practice and 4.5 offers a simple overview of the financial sector to explain the relevance of seeking data from varying sources. Web 2.0 technologies and user-generated content in the context of digital investigation are discussed in 4.6 before a description of the preparation necessary for safeguarding during online research (4.7). The search for a sample is sequentially recorded in sections 4.8 and 4.9 and 4.10 offers a reflection on the methods thus far. Section 4.11 concludes 'The Corporate World' and introduces the reader to Chapter Five, 'Executive Risk'.

4.2 A Technological Research Strategy – In Theory

This research was inspired by an incident occurring shortly before delegates from a multi-national financial organisation were to take part in a two-day crisis-management training programme. The organisation had requested a cyber-specific exercise and as an associate consultant, the researcher had liaised with data security managers to develop a cyber-incident scenario to test preparedness for business continuity after cyber-attack (see 4.3.4). The live exercise was to take place in London, delivered by expert providers in a state-of-the-art training suite using a team of role-players and real-time specialist software. When learning that the cyber exercise was based upon behaviours of corporate personnel, the chief executive officer (CEO) could not accept that employee digital

activity in the workplace might facilitate harm against the corporate network. Despite assurances of feasibility from the security managers who had assisted in creating the scenario, the CEO refused to consider the human element as a factor in theorised risk of cybercrime. His resolute faith in enterprise security convinced him that technological solutions would defeat any threat against IT infrastructure and employee activity need not be addressed as a risk to be mitigated. He suggested that the training exercise should instead feature a hacking attack against the corporate website conducted by perpetrators outside the organisation. After hasty modifications, the exercise was successfully accomplished.

The literature suggests traditional models of insider threat do not include the personal use of privately-owned technologies by contemporary employees as potential threat to workplace systems (Agrafiotis et al., 2015; Furnell and Clarke, 2009; Saxena et al., 2020; Ring, 2015; Warkentin and Willison, 2009). Threat assessments focus predominantly on external attackers and do not appear to factor employee digital activity as a contributor to cybercrime (BoE, 2016a; BoE, 2016b; BoE, 2016c; BoE, 2020; Fisher, 2015). To attempt to modify literature discussing insider threat, primary evidence from contemporary ‘insiders’ was required, and the investigation would focus on human behaviour, individual digital activity, and contemporary technologies. A sample of average users of technology would provide data regarding internet use, digital content, cyber awareness, and personally owned devices in and out of the work place.

The digital-led research strategy proposed that open-source internet investigation (see 2.3.7) would locate respondents to be personally invited to participate. Since

a key element of the study would determine personal internet use, the research design intended utilising internet presence of financial sector employees to ascertain suitability and find contact details for emailing the invitation. As described in 3.4.1, personal data and active footprints can be misused by an offender. Hence, the framework adopted by attackers when sourcing individual and organisational targets (Mouton, Leenan and Venter, 2016) would be followed and theorised risk of social engineering would drive the practical research. Search techniques would include “reviewing social media profiles and the online activity of potential targets” (Symantec, 2016, p. 33) combined with open access resources such as public records, government or public sector databases, and media archives.

Using the internet as a recruitment tool would locate individuals from assorted financial organisations as opposed to a large sample from a single company (Silic and Back, 2016). Respondents could be sought from varied locations, services, and corporate hierarchies. As the financial sector is a global industry, there might be opportunity to recruit UK and international participants offering opportunity for cultural comparison. Digital intelligence would find diverse subjects and allow scrutiny of generational, occupational, and gender-based differences and attitudes. Age was not significant, and it was preferable that all generations (except minors) were represented in the sample.

The open-source research was anticipated to identify two groups of potential candidates: (a) individuals known to be employed in financial services but with no indication of the company they work for, and (b) individuals who identified their

financial employer. Email addresses were expected to be found amongst published content and would be used to invite individuals from group (a) to volunteer. Any financial organisation identified from content posted by employees in group (b) would receive a separate invitation to take part and provide volunteers from the workforce. All participants would voluntarily complete an electronic mixed methods research instrument, designed to collect quantitative data and allow respondents to leave comments to open questions in the manner of an interview or focus group. The descriptive data would then be coded to allow evaluation. This quantifying of qualitative data (Strauss and Corbin, 1998, cited in Lapan, Quartaroli and Riemer, 2012) would enable inductive thematic analysis. The research questions and the cyber-RAT framework would theorise whether technological behaviour of average-user employees might be (in)advertently exacerbating risk of cybercrime.

4.3 Positionality and Reflexivity

Scholars suggest that a researcher should “reflect on their own philosophical stance” (Walsham, 1995, p.76, cited in Stahl, 2013) and define the viewpoint grounding each research study from the outset (Brown, 2015; Moon and Blackman, 2014, p. 1167). Since personal perspective of reality and knowledge acquisition may influence data interpretation (Brown, 2015; Thomas, 2004, p. 198) 4.3 will address positionality of the author as a digital researcher and acknowledge that personal values and ethics acted as a conduit for subjective bias. An ontology shaped by training in design is evaluated as a complement to the philosophical framework influencing the epistemological process. Personal values and ethical decision-making as a challenge to digital investigation will then

explain why this work offers three methodology chapters. Section 4.3 deviates from the previous third-person account as the self-reflexive nature of the discussion is better suited to a personal narrative.

4.3.1 The Human Phenomenon

The human element as a factor for technological victimisation in corporate space has been explored by academics and this work will add to other literature also using theoretical modelling. In particular, the worker as an aid to security via situational crime deterrent theory (Safa et al., 2019), strategy as practice to improve management policies (Choi, Martins and Bernik, 2018) and protection motivation theory in the context of compliance to mitigate insider threat (Johnston, Warkentin and Siponen, 2015). Shaikh and Oliveira (2019, p. 1) additionally propose a RAT framework and acknowledge "informal IT", referencing *some* of the personal technologies to be examined in this study. The authors do not include 'personal digital activity' and focus only on utility applications in a work-based capacity whilst proposing traditional RAT to improve organisational information security.

Silic and Back (2016, p. 36) advise that "business context" has not been adequately studied and investigation of the human factor (the employee) "may lead to better mitigation of the underlaying risks for organisations". This study intends to augment the proposal suggested by Shaikh and Oliveira (2019) and transpose RAT into the cyber domain, incorporating the liquid modernity proposed by Bauman (2000) to contextualise the fluidity of cyberspace. This re-imagining of the RAT model will evaluate the business context deemed so important by Silic

and Back (2016) and to enable a thorough investigation of the human factor, a data sample meeting exact specification is required.

4.3.2 Ontology in Design Practice

To locate an exact sample amongst thirty-nine million UK social media users (Johnson, 2020) requires an understanding of *where* to look but more importantly, *how* to look. I have undertaken training in Open Source Intelligence (OSINT) and Social Media Intelligence (SOCMINT) (see 2.3.7) to learn investigative search skills, but independent practice in open-source research has proved that an aptitude for abstract thinking is a necessary requirement. As a BA graduate in textile design and former freelance designer, I consider a capacity for creative thought to be an asset for digital investigation. Designers are constructive thinkers (Cross, 1982, p. 223) and design-thinking requires "pattern synthesis" as opposed to pattern recognition. A solution will not be "lying there among the data… it has to be actively constructed by the designers own efforts" (ibid.,1982, p. 224). When Cross's (1982) insight is applied to Bryman (2012) and the assertion that constructivism enables a researcher to "consider the ways in which social reality is an ongoing accomplishment of social actors" (Bryman, 2012, p. 34), it is apparent that the three research questions for this study are based in constructivist ontology.

A designers constructive thinking leads them to "learn about the nature of the problem, largely as a result of trying out solutions" (Lawson,1980, quoted in Cross,1982, p. 223). Thus, design-thinking can be observed in Chapter Two (see 2.7.2) and the "playing with theories" recommended by Wolcott, (2001, p. 81) as a

simile to the way that one plays with ideas. Examples to illustrate this are the re-imagining of preventative theory as a solution to theorise risk in a small-scale technological context and the suggestion that liquid modernity (Bauman, 2000) might explain the fluidity between players in a routine digital activity scenario.

The philosophy of constructivism considers the human factor as an essential element, necessary to apply subjective meaning and understanding to the individual social experience (Winston, 2012, p. 113). The ontological position of constructivism considers culture to be "an emergent reality in a constant state of construction and reconstruction" (Bryman, 2012, p. 34). This viewpoint encompasses the "designerly way of knowing, thinking and acting" (Cross, 2001, p. 55) which influences my perspective of research. Thus, having established constructivism as both the ontology and philosophical framework, a natural epistemology to complement a study of the human element using experimental methods, is interpretivism.

4.3.3 A Design Epistemology

The practical element of design requires observation of shape and form, and uses appealing elements of image, texture and colour as a framework to create something new. These 'fragments' of visual and tactile data are re-created in various formats, pieced together, realigned, and manipulated until the end product is aesthetically pleasing and recognisably complete. Finding the 'fragments', the inspiration which drives the creative process, uses interpretivist epistemology. According to the principles of interpretivism, the researcher is part of the research, interpreting data drawn from specific or contextualised environments, unable to be objective or removed (Brown, 2015). This transposes well to the concept of

working to a design brief, the instruction from a client informing what the finished image should represent, how it will be used, the expected colourway and the timeframe to produce the design. The specific or contextualised environment becomes the parameters of the brief and only subjective interpretation of the data observed within that space can resolve the search for inspiration.

The designerly way of knowing is observed in other industries where creative thinking is required to achieve a satisfactory solution in a minimal timeframe, for example architecture and engineering (Cross, 1982, p. 224). Instead of a scientific approach which focuses upon the problem (Lawson, 1980, cited in Cross, p. 223), a designer will achieve multiple outcomes focused upon the solution and reached by a process of synthesis (Cross, 1982, p. 223). A reflexive evaluation of the methodologies using design thinking as the model for the practical investigation, identifies that the 'brief' was to obtain a sample perfectly suited to the research parameters. The interpretivist epistemology as a method of achieving that outcome demonstrates that the combination of observed behaviours and analysis of user content was synthesised to identify ideally suitable candidates. The exploration of alternate resources illustrates a continuous re-thinking of the methodology, remaining focused on the solution.

4.3.4 Open-Source Research and Philosophical Frameworks

I became interested in the internet as an investigative tool during an MSc in Cybercrime and e-Investigation at University of Derby. The unpredictable nature of online research was appealing due to the requirement for continuous creative thinking. I later invested in open source intelligence training and practiced in a

freelance capacity using OSINT and SOCMINT (see 2.3.7) to complete diverse assignments for private organisations. Whilst practicing OSINT I became an associate consultant for a crisis and incident management company and in the role of cyber-advisor participated in live scenario-based exercises with teams from financial corporations (see 4.2). Study of cybercrime and OSINT, an awareness of preparing for unexpected events, combined with designerly creative thinking were significant factors in the design of this study, in addition to influencing the methods and interpretation of results.

Internet-focused open-source investigation also draws heavily on the constructivist perspective and a 'designerly' aspect. Interpretivism applies well as an epistemology for digital research where the brief defines the person, object, situation or circumstance to be sought, and the specific environment is cyberspace. The researcher is part of the investigation, applying subjective interpretation to the data obtained by observational inductive methods. If OSINT is evaluated as a process, using the 'designerly' way of thinking as a framework for interpretation, it is apparent that the practice begins with observations, develops into recognition and synthesis of patterns in data to detect themes, which are then explored to reach conclusions. Consistent with the design process, open-source research is focused on a solution, not a problem.

4.3.5 Subjectivity and Bias

A personal "worldview" may affect judgement (Goodson and Phillimore, 2004, p. 37) and preconceptions can influence analysis, results, and conclusions (Bryman, 2012, p. 39). Hence, a researcher must be reflexive and consider their own subjectivity, ethics, and values (Goodson and Phillimore, 2004, p. 34) as the

subjective component of interpretivist epistemology is likely to introduce an element of bias. Subjectivity may be a positive attribute in the context of textile design as it can assist with achieving an aesthetic outcome. As the creator of a piece of work I will naturally have bias towards elements I find visually pleasing and am unlikely to include those that do not appeal to me artistically. Subjectivity may also be positive during open-source research where personal bias regarding internet behaviour may contribute to the investigative process. In regard to this study, personal bias may have a negative effect as I acknowledge that the conclusion to (mis)use of technology will be influenced by my own principles as someone who has studied cybercrime. The positive aspect is that findings affected by subjective bias may deliver objective theorised threat intelligence.

Personal bias impacting on interpretive methods is easily linked back to OSINT training where the necessity for safeguarding personal privacy, footprints and digital systems is enforced by practical application of protective processes. Internet research entails considerable hours in cyberspace, and I am often positioned to recognise suitable target and areas for guardianship. By self-reflecting on personal values, I now recognise that the unjust consequence of a user's actions (or inactivity) causing negative impact to other entities was a significant factor in the design and evolution of the central investigation. Where guardianship qualities are lacking in average users, others may have to assume protective roles, and in the workplace, these will be the representatives of the organisation. It is equally unjust that average users are unaware how frequently they become suitable target during routine digital activity. Basic awareness might enable capability as guardian, but a user lacking knowledge may always be a

suitable target. Hence, objective threat intelligence delivered by the subjectively analysed results is as much for the benefit of the employee as the employer.

4.3.6 Ethics and Internet Research

Due to the dynamic, volatile, fluid nature of the internet discussed in Chapter Two (see 2.4), using online facilities as an intelligence tool can present unique ethical dilemmas with no structured parameters. The academic debate regarding decision making in a digital context rightly centres on informed consent and includes authors of online content (Burles and Bally, 2018), whether an online community constitutes public or private space (Roberts, 2015) or sensitive user-generated content as private or publicly accessible (Eysenbach and Till, 2001). As a consequence of the capricious nature of digital research, a 'fixed' ethical framework is not sustainable. Guidelines applicable at "one point in time" cannot be expected to apply to "current and future online environments" (Roberts, 2015, p. 322). Internet research should therefore be guided by "general ethical principles" (Roberts, 2015, p. 322) including "researcher reflexivity and sensitivity to the online context" (Whiteman, 2012, cited in Roberts, 2015, p. 322). This parallels the viewpoint of Markham and Buchanan (2012, p. 5) who advocate an inductive approach to decision making and advise that "harm, vulnerability, respect for persons and beneficence" should remain a constant focus. Thus, a digital researcher accepts that constant due diligence and continual ethical decision making is a part of the online research process.

From a philosophical perspective, my open-source research follows interpretivist methods of knowledge acquisition, hence, due diligence in digital research is a subjective response occurring whenever personal values are threatened in an

ethical context. Academic research is constrained by adherence to the guiding principles in the University of Derby Research Ethics Policy and Code of Conduct (University of Derby, 2011) and due diligence in academia requires personal interpretation of non-malfeasance. My master's thesis documented an exploratory investigation of social media as a resource for recruiting a sample and experienced the largely unwritten (though enforceable in practice) etiquette of the networked community. This dictates not abusing online spaces for marketing or spam and administrators and other users act as gatekeepers (Hooley, Marriott and Wellens, 2012) to challenge, report or block those who break the rules of 'netiquette' (Hodges, 2002). Prior experience with gatekeepers exacerbated my response to malfeasance which was already subjective towards my personal values in digital activity. For example, I am zealous with privacy controls, do not invite user interaction and any unsolicited contact is deleted immediately. In professional practice I use the industry recommended safeguarding solutions described later in 4.6 and only accept commissions from trusted sources. Thus, my determination to not cause harm, particularly in respect to a user's privacy, provoked a quandary which impacted on the resolution of the practical research recorded in 4.8. My personal values entailed that use of internet messaging facilities was not acceptable to promote academic research. A user may feel that privacy had been infringed and that rules against spam had been breached. The consequence of this ethical dilemma forced the methodology to change direction and enter a second chapter.

4.3.7 Three Methodologies for Digital Investigation

Eysenbach and Till (2001, p. 1103) discuss three categories of online research: passive data analysis, active data analysis, and the internet as an instrument to

execute qualitative methods such as interviews, surveys and focus groups. In these three categories, the internet is the primary method of data collection and the information obtained is analysed for the subsequent results. A further use for the internet as a research tool is to recruit a sample for “traditional” research (Eysenbach and Till, 2001, p. 1103). An example of this may be a request posted to an online forum to seek volunteers to complete a survey.

The methodologies recorded in this thesis document a further example of digital research, where user data is not analysed to produce results but evaluated to determine respondents meeting specific characteristics for an investigation. The methodology chapters highlight how digital research can be unpredictable and does not adhere to a research strategy. The constant requirement for reflexive due diligence requires a researcher to be flexible, tenacious and prepared to deviate from preconceived proposals. The remainder of ‘The Corporate World’ will illustrate that despite many potential candidates, ethical constraints prevented a successful outcome. Thus, the determination to recruit an ideal sample pushed the methodology in a new direction and Chapter Five, ‘Executive Risk’ will demonstrate how users demonstrating specific traits encouraged financial organisations to participate. Chapter Six, ‘A New Direction’ deviates still further from the original research strategy but continues to maintain the premise of an ideally suited sample.

4.4 The Research Strategy – in Practice

Section 4.1 described the research strategy as it was designed. In practice, the investigation was experimental, demanding reassessment of preconceived ideas,

constant improvisation, and exploration of unfamiliar online platforms. During data collection it became necessary to modify the focus of the search, taking the investigation in a new direction. So that the reader might follow the inductive decision-making process as it occurred, all three methodologies are recorded as individual chronological sequences on a pathway to data collection. The findings from the applied methods are significant to cyber-RAT and suitable target seen in **RQ1 actual/perceived risk, RQ2 average usage/impact** and **RQ3 IoT unexplored risk**, thus a detailed narrative is necessary. Signposting throughout the chapters will direct the reader to other resources or offer additional clarification. The remainder of 'The Corporate World' will discuss preparation and preliminary steps and final execution of the search for individual employees. As each methodology seeks respondents from different sectors, section 4.5 begins with a brief overview of the financial industry to clarify the position of respondents as sector employees.

4.5 The Financial Industry: A Brief Overview

In simple terms, the structure of the UK financial industry is a collection of commercial institutions assisted by economic support services. These are overseen by a central bank providing regulation and supervision to a number of corporations and services. Other organisations are superintended by an external regulator. Unresolved disputes between consumers and financial businesses are determined by an independent decision maker. Customers are protected from instability and failure experienced by a financial business by an independent compensation scheme (Bank of England, 2019a). To accompany the official

regulatory structure, a range of professional bodies represent each of the institutions and services.

To place this in context, banks and building societies provide commercial ‘money management’ supported by thousands of firms providing services and selling financial products (Financial Services Compensations Scheme, 2019). These include accounting, insurance, investment and financial planning (Higginbotham, 2018). The Bank of England is the central bank, and provides prudential regulation to banks, building societies, insurers, credit unions and major investment firms. The regulatory service is delivered by the Prudential Regulation Authority who supervise approximately fifteen hundred organisations (Bank of England, 2019b). All other financial service providers are regulated by the Financial Conduct Authority (FCA, 2016) who are responsible for the conduct of more than fifty-eight thousand (58,000) businesses. These include financial planners, mortgage brokers, investment services and wealth management. The trade organisations representing financial services include chartered organisations, institutes and associations who support and assist professionals employed in each sector of the industry.

The Financial Ombudsman is the independent public body assigned to resolve disputes between consumers and financial businesses by taking an unbiased view of any unresolved issue to find in favour accordingly. The organisation is equipped with legal powers to correct any prior decisions made during disputes. Decision-makers at the Ombudsman come from diverse backgrounds, including police and border patrol, legal services and academia in addition to financial

professionals. The narrative recording the methodologies will establish that 'The Corporate World' (methodology one) and 'Executive Risk' (methodology two) focus exclusively on commercial corporations involved in money management. Segment 1 (6.2) of the third methodology ('A New Direction') incorporates a variety of financial services and the final stage of data collection (Segment 2, 6.6) includes financial regulatory bodies.

4.6 Web 2.0 as a Resource for Open-Source Intelligence

Web 2.0 technology has created many outlets for individuals to publish personally generated content and invite other users to interact by sharing, liking or contributing comments. Blogs (web logs), podcasts, vlogs (video blogs), image sharing and social networking sites like Facebook, LinkedIn, Twitter and Instagram are all examples of Web 2.0 technologies. These platforms encourage billions of users to deposit vast quantities of personal information onto the internet. To illustrate with context, in a single day Twitter will generate approximately four hundred and eighty thousand tweets, and sixty thousand images will be uploaded to Instagram (Nodegraph, 2020). For the open-source investigator, Web 2.0 technologies provide a stream of valuable data which can be accessed and organised using a variety of tools and techniques. Many of these tools are free and available on the internet, others are purchased by subscription. For the purposes of this academic research and to follow the requirements of the Research Ethics Policy and Code of Conduct (University of Derby, 2011) only legitimate, free, credible and publicly available resources would be utilised for this project.

Normative online searches would take place using the Google search engine and facilities for enhanced searching such as Google Advanced Search. These would include Boolean techniques where operators OR, AND, or NOT are attached to keywords to create strings of search terms. Google Advanced Search and settings available on the Google home page allow parameters to be set when searching through specific sites or time frames. No unethical or illicit methods would be applied including 'data mining', 'extraction', 'scraping' nor any automated services. Open-source tools would be used only for the purpose of identifying data patterns or themes. User-generated content on social media sites would only be viewed if a user's profile or any belonging to the associated network were unprotected by privacy controls and visible to any internet user. No requests would be made to 'friend' or 'follow', nor would any content be 'liked' or commented upon to initiate or incentivise communication. This was particularly relevant as the researcher would conduct all online research using a fake identity. Standard OSINT investigatory practice is to use social media profiles in alternate names to protect law enforcement or other agents. In the context of academic research, a false identity would safeguard against over-exposure on the internet, but as discussed in 4.3.6, avoiding malfeasance (University of Derby, 2011) was a guiding principle to the researcher. To initiate contact with another user whilst using a fake identity would be a deception, and constant due diligence would ensure that nothing untoward took place. The process taken to create a fake user profile is explained in 4.7.

4.6.1 Social Media Users as Assets to Academic Research

Crossler et al. (2013, p. 96) suggest that people are unwilling to admit to behaviours which might be considered as unethical. Thus, procuring data regarding *actual* conduct is a challenge faced by academics studying behaviours in information security. Nonetheless, the literature references narcissistic tendencies in users of Web 2.0 technologies (Bergman et al, 2011; Carpenter, 2012; Wang, 2017) and some social media users achieve status as 'influencers' (Freburg et al., 2011; Khamis, Ang and Welling, 2017; Ormerod, 2018). Candid videos, 'selfies' and forthright opinions placed into the public arena invite others to pass judgement on subjective content considered meaningful by the user-publisher. Thus, it is possible that self-promoting users who are unperturbed at divulging personal information may be candid when answering 'sensitive' questions. Recruiting participants identified by prominent use of social media may therefore grant access to otherwise unattainable data.

A sample of two hundred employees would provide sufficient empirical evidence to identify implicit trends in user behaviours, and by utilising web resources and open-source techniques suitable candidates could easily be identified. If these social media users are self-promoting or influential, they may include email addresses amongst their published content. In contrast to Hodgkinson (2008) who devised a research instrument on assumption that the sample was busy and time-poor, this study anticipates that individuals recruited via social media will enjoy taking time to talk about themselves. Accordingly, the questionnaire provides opportunity for respondents to elaborate on personal circumstances.

The average response rate for web-based surveys is alleged to be thirty-three percent (Lindemann, 2019; McRobert et al., 2018) and a badly designed or vexing survey is liable to be abandoned before completion (Peytchev, 2009 cited in Dodge and Chapman, 2018). It is hoped that a personal invitation and an enjoyable survey experience might encourage a higher percentage of completed submissions. If responses are low, a seventy-five percent return rate from a purposive sample would still be sufficient for thematic analysis. If insufficient samples were completed, further online searches would likely find other suitable candidates and the invitation process could be continued. In 4.2 it was theorised that in addition to those who did not identify their employer, the investigation may locate individuals who name the company they work for. The intention was to invite any identified organisation to provide volunteers for participation. If this proved a successful method for recruiting many volunteers from a large organisation, a thirty-three percent response rate would be sufficient.

Foddy (2011, p. 117) advises that “question threat” can hinder responses as intimidating questions may cause alarm. The research instrument did not intend to threaten, but a respondent might recognise personal behaviour and realise that digital activity may incite harm. Subsequently, question threat may impact on a truthful answer. Nonetheless, the networked community is a contemporary phenomenon and active members are familiar with making content available which may be personal in nature and offering opinions to be critiqued by others. Recruiting a social sciences sample via internet resources may obtain respondents with a different outlook to those acquired through traditional methods. Questions requiring input as personal comments may fit the narcissistic

framework epitomised by social media. An enquiry which might intimidate a respondent in a face-to-face interview situation may be insignificant to a user with an active presence on multiple social media platforms.

4.7 Safeguarding Preparation for Online Research

Routine internet use leaves an inadvertent trail of data which can be used to identify a user or to track online activity (see 2.3.2) Additionally, when a user visits a website, their devices or system will supply data about their settings, internet protocol (IP) address and location (Table 1, 2.3.3). Standard open source practice recommends specific controls to prevent leaving data which may be associated with an investigator. This section (4.7) describes the safeguarding measures to be employed during this research.

4.7.1 IP Addresses

The practical research would not take place in an educational establishment and the viewable IP address would be for a residential address and not the one associated with University of Derby. Open-source investigators use the Tor browser (see 2.5.2) to safeguard against an IP address revealing a location. Tor uses layers of encryption and multiple servers to hide a users' locale and any observer monitoring web activity will see only a connection to the Tor network (Tor Project, 2020). If Tor is used as a standard web browser it can impede download speed since web traffic must be relayed to several servers. Investigators are advised to install the Tor browser onto an external storage device and the portable browser may then be used whenever necessary. Downloading Tor to a portable flash drive initiated the research process.

4.7.2 Footprints and Fake Identities

The digital investigation would utilise well known social media platforms such as Facebook, Twitter and LinkedIn and would also explore sharing economy sites, social discovery apps and other messaging services as potential sources of data. The research design proposed that standard OSINT protective measures be enabled since access to a diverse range of sites and services may leave a trail of active and passive footprints. To safeguard against digital activity being associated with the researcher, the University Research Ethics Committee granted approval for the creation of fake identities. These would be used to register for any online accounts and user profiles.

The free service Fake Name Generator (https://www.fakenamegenerator.com) was used to create two random female identities. 'Laura' and 'Charlotte' would enable access to websites and applications during the practical research and each required an active email address to verify registration. Although web-based software is available to create a temporary self-deleting address for verification purposes, permanent email accounts were necessary for frequent access. GMX Services (http://www.gmx.com) provided web-based email for both identities. The registration process for some websites required nothing more than the fictitious names and dates of birth, while others demanded extensive information. Whenever personal details were necessary, the researcher elected to supply factual data such as her own tastes, values, and opinions. If a profile picture was required, neutral images of flowers or plants from a personal photograph collection were used. The images had no geolocation tags and metadata would only identify the apparatus used to produce the image and the date of production.

4.7.3 Social Media

In addition to maintaining family or friendship groups, social media is a major platform to reach customers and established brands and corporations, small business owners, self-employed or freelance workers promote themselves and exhibit their work. A further recent concept of contemporary society is to consider oneself as a 'personal brand' (Rosser, 2017) and social media provides the perfect medium for millions of individuals to endorse their 'brand' and indulge the narcissistic desire to be 'followed' or considered as an influencer (Freburg et al., 2011; Khamis, Ang and Welling, 2017; Ormerod, 2018; Wang, 2017). Thus, promotional profiles generally encourage user engagement and a variety of methods including email and social sites are offered to interested parties wanting to initiate communication. The research design anticipated identifying 'self-promoting' financial sector employees and expected to find email addresses amongst published content. The correspondence inviting the individual to volunteer would truthfully state that the user's content had been viewed and that it was pertinent to the study. It was hoped that those who aim to influence others would conform to the model of narcissism associated with social media and consent to participate.

The 'Charlotte' identity was used to create accounts on Facebook and Instagram consisting of the username and a profile picture of a flower. No other personal details were provided. 'Charlotte' would be used to search for financial industry employees, and it was expected that social network algorithms would begin making recommendations based on the content viewed and accessed. Other users working in finance might be proposed as potential friends or followers and

could be evaluated for suitability as candidates. Notifications would be sent to 'Charlottes' email address, clarifying the preference for a permanently accessible account instead of a disposable option.

The fake profiles were created solely as an instrument to facilitate safe searching and no social media methods would be used to initiate contact with a user recommended by an algorithm. Nonetheless, it is worth noting that after the Facebook profile was activated, it remained dormant for four days before any search activity took place. Despite this, the profile received fourteen unsolicited 'friend' requests. The Instagram profile was inactive until the Facebook research was in progress but began receiving regular notifications to say that people were 'following' the profile and 'Charlotte' was invited to follow them in return. This illustrates the ease with which social media can solicit connections between individuals. In the context of cyber-RAT, social media users may be suitable targets, not only from accessible content unprotected by privacy enhancing technologies such as privacy controls, but by accepting friend requests from unknown senders. As explained in 3.4.3, digital systems affected by malware can imitate humans and distribute friend requests as a method to spread malicious code (Symantec, 2016). Older or other vulnerable users may be particularly at risk of becoming 'friends' with unknown entities and effective guardianship may only be enabled with enhanced awareness.

4.8 Preliminary Steps

Ordinarily, an OSINT search for an individual will commence using basic details already known, for example a name, address and date of birth, or a name and

geographical location of work or residence. For this research, unknown users were being sought and the only prior knowledge was employment in the financial sector. The investigation began by exploring the sector to ascertain occupations, qualifications, industry bodies, areas of commercial operations and primary stakeholders. Websites offering careers and employment advice to university graduates were perused to identify organisations with a substantial UK presence. Graduate services were of variable quality and those targeted at generic students as opposed to specific university careers offices were the most useful resources. These sites identified universities renowned for supplying graduates to the financial sector, the top graduate employers and names of professional bodies supporting the industry. Employment services were then used to compile a list of forty-four financial occupations. Facilities for policy makers (The City UK, 2017) provided information about key financial areas in the UK market. Twenty-two international financial districts were identified using Google UK and fifty-one UK towns and cities were seen to have a large concentration of financial corporations.

The financial occupations, towns and cities were used as keywords in Boolean searches to detect names of organisations with those positions in the corporate hierarchy. The corporate names were then used to obtain annual reports and PDF documents published online. Many businesses submit annual paperwork, and some reports are available to view on a corporate website and others must be found by dynamic deep web searching. When conducting a search to retrieve archived documents, varying permutations of search terms can return different results, so many combinations should be tried for the best outcome. Once reports were retrieved, searches were conducted inside the documents. Finally, online

directories and Google UK obtained the location of company headquarters and major enterprises. A list was compiled of one hundred and fifty-three (153) banks, building societies and other financial organisations.

4.8.1 Financial Organisations

The organisations were entered individually into Google as keywords. 'Hits' (search results) were returned for corporate websites which were examined individually to seek names of any employees and to identify the format of the company email address. Names and emails were then recorded for use as key words. An account was created for Endole (http://www.endole.co.uk), a free service to conduct due diligence on organisations and associated staff. Endole offers an 'explore' tool with filters to search through service activities. Using the filter "Financial Service Activities except insurance and pension funding" returned more than ninety thousand (90,000) financial organisations. Companies with a minimal net worth were disregarded and brief searches were conducted on the remainder to identify whether an active website was available where names of employees might be found. It was noted that many organisations provided substantial information about staff members including a job resume, accreditations and personal biography revealing hobbies, interests, hometown, or name of partner. Significant words were recorded for key word searches.

4.8.2 Professional Bodies and Industry Databases

The names of professional bodies and an operator to locate PDF documents were entered into Google Advanced Search, returning 'hits' relating to archived presentations hosted by the professional body. Information about the presentation was accompanied by a list of attendees and the names of their

corporate employers. Each organisation was investigated using Endole to find the active website. The London Institute of Banking and Finance was returned as a 'hit' as the website contains a register of alumni who have obtained professional qualifications. Access to the membership and alumni areas of the site were password protected, but a database holding the register was not. To search for an individual entry on the register, one letter from the first name and two letters from the surname had to be entered into the search fields. The database would retrieve all names corresponding to those letters. Experimental searches were conducted using A' in the field for the first name and the letters 'BR' (to represent Brown), 'SM' (Smith), 'WI' (Williams, Wilkinson, or others) and 'CO'(Collins) in the surname field. This returned several names and places of employment. Searches were repeated using 'B' and then 'C' for the first name and the same series of letters for the surname and retrieved ninety-eight names and associated workplaces. The same method was applied to an online database hosted by the Institute and Faculty of Actuaries which added a further thirty-five names to the list of potential candidates.

4.8.3 Dating Sites

Dating sites pair individuals with similar interests and values and require users to provide significant amounts of information so that suitable matches can be made. Subsequently, OSINT investigators find dating websites to be a valuable resource for personal data. Sites vary in quality with some providing free services and others requiring users to purchase a subscription. As the remit for the practical research was to utilise only free open sources, the 'Laura' identity was used to create a profile on OK Cupid (http://www.okcupid.com). Privacy controls were

activated so that ‘Laura’ could not be found without effort, although complete concealment was not possible.

The onsite search facility enabled searches to take place for individuals in specific occupations rather than industries and the available categories were ‘technical’, ‘clerical’ and ‘managerial’. The first search returned many results, but it was not possible to confirm employment in the financial industry without initiating contact with applicable users, rendering OKCupid as unsuitable for the research. ‘Laura’ was deleted from OKCupid, and a new profile created on Telegraph Dating (http://www.dating.telegraph.co.uk). This site had potential as a source of intelligence as users could seek a prospective partner with an occupation in a specific sector, and a preliminary search for financial services returned one hundred (100) usernames. Whilst recording the usernames for further research, the ‘Laura’ profile was logged out of the website and the username and password were not recognised when attempting to log back in. Attempts were made to reset the password via email but were unsuccessful and ‘Laura’ had to be deleted and a new account created for ‘Charlotte’. The search for ‘financial services’ was repeated, and the dating profile of each search result examined individually. All retired, self-employed or independent financial advisors were removed, and thirty more usernames were added to the list of potential candidates.

“UK dating sites with keyword search facility” was entered as a search term into Google UK and a ‘Charlotte’ profile was subsequently registered on Freedating (http://www.freedating.co.uk). A keyword search for “financial services” returned two hundred and thirty-four (234) usernames. Each profile was examined to

remove any retired, self-employed or independent financial advisors, and any user with insufficient personal data to create keywords. Fifty names and locations were added to the list of potential candidates. A final search using “Canary Wharf’ as a keyword found one user who worked for a financial company in Canary Wharf who was added to the list.

4.8.3.1 Reflection on Dating Sites

The value of a dating site to open-source investigation was evident, but for this project the intrinsic design of a dating site was a limitation. When a profile is created, the user must specify the gender of suitable matches and for ‘Charlotte’ the default preference was set to ‘women seeking men’. All in-site searches thus returned profiles from users identifying as male. To recruit a gender balanced sample, it would be necessary to either create a male identity and conduct a similar search for female employees or re-configure ‘Charlotte’ so that the default preference became ‘women seeking women’. If dating sites proved successful in recruiting a male sample, the modified searching mentioned above would take place. If not, dating sites would not be used again in this investigation.

4.8.4 Keywords and Site or Domain Searching

The string “Accounts Manager" OR "Financial Analyst" OR "Auditor" OR "Budget Analyst" OR "Loan Officer" OR "Accountant" was entered into Google Advanced search. The word ‘jobs’ prefixed by a NOT operator was added to prevent employment opportunities posted to recruitment sites returned as hits. The term "Canary Wharf" was added to the string as this location is a major financial centre and the base of several global head offices. Google was modified to search only

inside the domain “LinkedIn.com” and pages in English were requested. The search returned ten pages of users matching the search criteria.

The users were either employed in financial organisations located in Canary Wharf and or employed in the locality of Canary wharf and included as their work histories matched the search terms. Those not currently employed in finance were removed in addition to senior level corporate staff such as directors, presidents, chief executive officers and similar. The investigation was focused on finding users with an active personal social media presence and it was assumed that senior personnel in Canary Wharf may have limited time for personal social media use. The remaining names were added to the list of potential candidates.

4.8.5 Instagram

The majority of user-generated material available on Instagram is visual, consisting of images and video. Other content is created by users posting comments as captions to accompany images or media files, or responses from those who have viewed content. Text-based content is typically supplemented with hashtags (#) which categorise information and enables searches for trending or popular topics (Moreau, 2016). Keyword searches were attempted using the Instagram search facility and a combination of search terms, for example “people who work in finance”, “employees in finance” and “employees at financial corporations”. These terms returned corporate profiles for financial organisations or pages intended for employees from specific corporations. A search was made using hashtags including “# I work in finance”, “# I work at Canary Wharf”, “# working in London” and “# working at…… a financial brand name, for example

Barclays, Lloyds, HSBC and others. The hashtag "# I work at a bank" returned several 'hits' leading to users who had posted photographs from the workplace, illustrating their employment. This has relevance to **RQ1 actual/perceived risk** and as the images are likely to have been taken using a mobile device, these users are additionally relevant to **RQ2 average usage/impact**. One employee had posted a photograph of her staff handbook identifying the name of her financial employer and disclosing her real name rather than an Instagram username. This is another example relevant to **RQ1 actual/perceived risk** and **RQ2 average usage/impact.** A Google search using the real name retrieved a LinkedIn account, thus demonstrating suitable target where lack of guardianship might instigate a social engineering attack. In regard to this investigation, prospective candidates found on Instagram offered no methods to initiate contact other than the facilities provided by the social platform. No personal email addresses were found amongst users' content.

4.8.6 Real Time Social Search Engine

A real-time social search engine (http:// www.social-searcher.com or http:// www.socialmention.com) allows the user to input search terms and the software scans through multiple social media sites to find recent posts which match. These search engines are an asset to brands and corporations seeking to gauge customer satisfaction or reputation. Searches using keywords related to financial services returned multiple 'hits', but on further investigation each 'hit' tended to be an interested commentator rather than an employee from the financial industry. As a tool to locate unknown individuals from random keywords, a real-time social

search engine was not satisfactory, but the value was evident as a useful facility for an investigator monitoring social media content.

4.9 The List of Potential Candidates

The list of candidates included nicknames, male and female first names and complete names (forenames and surnames) supplemented with a combination of letters or numbers. Some names were supported by additional data including location, job title, names of employer or hobbies and sporting interests recorded to be used as keywords. In respect to **RQ1 actual/perceived risk**, the data users make available online indicates suitable target at risk of social engineering conducted via Web.2 technologies. The candidate list was filtered to remove all executive level staff and the remaining occupations included middle management, supervisory staff, team leaders and frontline positions such as clerks, officers, associates and administration. The purpose of the next part of the investigation was to locate a contact email address to be used to invite the potential candidate to take part as a volunteer.

4.9.1 LinkedIn as a Resource

Open-source practitioners are routine users of the LinkedIn social network site for professionals as significant information can be viewed on profile pages and used to generate further investigation. Consequently, offenders planning social engineering attacks may also find LinkedIn to be a valuable resource and in respect to **RQ1 actual/perceived risk**, employees who make substantial personal data available to a public audience may be a suitable target. Profiles may be viewed after logging into a personal LinkedIn account and unlike other social

networks, notification is sent to a user whenever their profile is accessed. Premium (paid) services allow account holders to see the identity of anyone who has viewed their profile, an advantageous facility for those seeking employment or business opportunities.

OSINT investigation advocates browsing within LinkedIn without activating notifications to alert a user that their profile has been viewed. LinkedIn privacy controls only conceal identity, not viewing activity and a researcher or investigator with full privacy enabled will still alert a profile holder that their page has been accessed. To avoid triggering alerts, OSINT practitioners use Google Advanced Search to seek specific terms within the LinkedIn.com domain and any returned links to profiles are then accessed using a standard web browser, circumventing the login procedure and enabling anonymous browsing. The names of potential candidates and the accompanying data were used as individual keyword searches using Google UK, and if results indicated an active LinkedIn account, Google Advanced Search was used to view the profile. For the first part of the investigation this method worked well but eventually an anomaly was observed. Google Advanced Search could return user profiles, but it was no longer possible to access them via the web browser; the LinkedIn log-in page would load by default instead.

It is very common for open-source tools and techniques to cease functionality without warning. An upgrade or modification to a website may cause a valued resource to disappear and OSINT practitioners regularly post information onto websites or blogs to advise when familiar methods have ceased, and new ones

identified. A simple Google search querying LinkedIn revealed that the social network had recently amended the on-site search facility, subsequently disabling the feature facilitating anonymous browsing. A post on an OSINT blog recommended entering the hyperlink for a LinkedIn profile into an online language translation service. Changing the language modified the web address and re-enabled anonymous browsing. The user-profiles were examined to ascertain whether links to other social media profiles or personal blogs were embedded in the content. Personal information was used as keywords in searches to locate other accounts maintained elsewhere on the internet.

When other accounts were found, the username was used as a search term. This retrieved comments posted by the user and images where they were 'tagged' to other people's Facebook content, revealing connections between the potential candidates and their social network. The Facebook site has a facility where the unique ID number allocated to every profile can be used to search for categories of data available on the social network. This includes photographs taken by the subject, of the subject, commented upon by the subject and multiple other options. The Facebook ID number is present in the source code of a social media profile and accessed by performing a 'right click' inside the profile page. Open-source tools (freely available on OSINT websites, see https://www.toddington.com and https://www.uk-osint.net) can match the ID to data distributed throughout Facebook. This method collected copious amounts of personal information and identified family and professional relationships, demonstrating relevance to **RQ1 actual/perceived risk** and suitable target without guardianship. Nonetheless, no methods of establishing communication

were identified from any of the profiles viewed, other than those provided by the social platform.

4.9.2 OSINT Techniques

If a profile photograph of a potential candidate was available, the image was copied and pasted into an image search engine so that a ‘reverse image search’ might be performed. This technique treats the image as a search query and the engine searches the web for other photographs with the same qualities. The search engines used for this research were Google Images (https://images.google.co.uk) and TinEye (https://tineye.com). Searching by image identified friendship groups and other work colleagues in the financial industry but did not find any personal websites or blogs where alternative communication methods might be available.

When the usernames collected from dating sites were used as keywords, it was noted that many were unique, most likely created specifically for the dating site. These names appeared nowhere else on the internet and had to be eliminated from the list after repeated failure to return ‘hits’. Those consisting of forename and surname with attached numbers or letters had more success when entered into a people-specific search engine. These free tools explore vast quantities of online data and identify ‘traces’ of profiles or accounts (see 5.3.1 for explanation about online tools used for open-source investigation). People-search techniques aided compilation of information about some of the potential candidates, including ‘wish lists’ of items on shopping sites, interviews or references in online media sources and attendance at industry events. Data of this type was superfluous to

this investigation, but from the perspective of a social engineer any information which might convince a victim of credibility is of value and in accordance with **RQ1 actual/perceived risk** may position a user as a suitable target.

By making use of two people-specific search engines (see 5.3.1) advanced search techniques and reverse image searching, other dating site accounts were retrieved where individuals had used an identical username or profile picture. Personal information posted in the dating site biographies suggested that many of the potential candidates would have been ideal for the research project, but no external method of establishing communication could be obtained. Dating sites offer various communication systems for account holders including internal email, direct message, initiating live 'chat' if the other party is online or use of visual icons to demonstrate interest. None of these methods were appropriate to issue an invitation to take part in the research project. As described in the discussion of ethics and personal principles (4.3.6) use of internet messaging facilities was not acceptable due to fear of malfeasance. More importantly, misleading dating site users hoping to meet new acquaintances would contravene the ethical values of the researcher.

4.10 Reflection

Although the objective of procuring email addresses failed, as an exercise in theorising suitable target, methods in 'The Corporate World' were a success. Employees provide substantial amounts of personal data and user-generated content was observed on public sites with no privacy controls in place. This was particularly evident on accounts held by users displaying narcissistic tendencies

(Bergman et al, 2011; Carpenter, 2012; Wang, 2017) where abundant self-portraits intended to evoke responses from other users (Wang, 2017) were publicly accessible. In accordance with **RQ1 actual/perceived risk,** this may position a user as suitable target with data at risk of exploitation by social engineering or misused to prove credibility in an attack against another in the user's personal network. In the context of **RQ2 average usage/impact,** selfies taken with mobile devices contribute to exploitable data, and when used to access social media in the workplace may be a risk to an organisation. Viewing the search results through the lens of cyber-RAT places social media users in position of suitable target and lack of capable guardianship finds organisations at risk of convergence. Retrieved content explicitly demonstrated that users are employed in the financial sector, and many of them identified their corporate employer (**RQ1 actual/perceived risk)**. To illustrate this with context, a user on the candidate list provided images of their recent society wedding, 'tagged' family members in the wedding photographs, posted 'tagged' images of college friends and linked online media coverage of the wedding to their own and acquaintances social media profiles, none of which had guardianship in the form of enabled privacy enhancing technologies. This user identified Goldman Sachs as their employer and their place of work as New York. An attacker could use the personal data to manipulate the user into accepting them as a social media friend, thus granting access to the user's evidently influential network. Sufficient information was available to create credible phishing emails which could be sent to either a social media email address or a generic work email thus placing the organisation in position as suitable target.

None of the prospective candidates provided any personal contact details and only three corporate email addresses were retrieved during the investigation. If sufficient company email addresses had been found then sending the invitation to a corporate account may have been considered, despite the risk of interception by spam filters. All the employee social media profiles had facility for communication between users, but direct messages would not be used. Not only were the researcher's profiles fictitious and any communication would be tantamount to deception, promoting academic research would be content consistent with spam. A possible solution may have been for the researcher to create social media accounts in her own name and send a direct message to each suitable candidate using the social network they appear to use most. Nonetheless, it must be considered how an unsolicited message may be construed. Users may consider the researcher to be engaging in inappropriate monitoring if an attempt was made to interact via the direct message facility on a profile page. As the invitation to take part would have included all the relevant details about the project, a disgruntled user may have felt justified in making an official complaint to the University of Derby or notifying a gatekeeper of attempted marketing. A complaint or ban would affect the researcher's credibility and possibly create a passive footprint to remain online indefinitely. Although the issue of deceiving users may have been avoided by use of an authentic profile, it was preferable for the researcher to remain unidentifiable, despite the limitations encountered for initiating contact with potential candidates.

4.11 Conclusion to 'The Corporate World'

The research design described in 4.2 of 'The Corporate World' was approved by an independent university ethics committee to utilise the internet as a tool for gathering open-source intelligence. Web 2.0 technologies and publicly accessible user-generated content were to be employed as resources to recruit a sample ideally suited to the parameters of the research. **RQ1 actual/perceived risk, RQ2 average usage/impact** and **RQ3 IoT unexplored risk** were to be considered in the setting of the financial services workplace. Thus, digital investigation would seek financial services employees using methods employed by social engineers sourcing targets framed in theoretical cyber-specific RAT**.** Unlike typical open source investigation beginning with a named and identifiable search subject, research methods began with exploration of online resources to identify users with a connection to financial services (see 4.8). The research strategy (4.4) predicted that employees who were avid social media users would be easily located. Over two hundred potential volunteers were identified, and content examined for external contact methods (4.9).

Evaluating digital investigation in the context of cyber-RAT, identifies OSINT and SOCMINT (2.3.7) as passive and active footprints left by routine digital activities, placing users as suitable target at risk of convergence. Mimicking the actions of an attacker using the social engineering framework (Mouton, Leenan and Venter, 2016) achieved the objective of identifying average-user financial services employees. Significance to **RQ1 actual/perceived risk** was evidenced prior to any primary data collection and in light of user predilection for mobile social networking (3.9.4) content may have additional value to **RQ2 average**

usage/impact. Nonetheless, failure to obtain a method of inviting candidates to volunteer for the project prevented progression towards data collection. The aspiration that employees might be 'influencers' or publishing content inviting external communication was unfounded. Subjective ethical decision-making and concern that user-perceived inappropriate monitoring might contravene ethical principles (University of Derby, 2011) prevented use of messaging systems available on social networks. The outcome of Chapter Four demonstrates that although methods were effective at finding suitable candidates, the strategy was ineffective at sample recruitment.

'The Corporate World' illustrated how **RQ1 actual/perceived risk** and **RQ2 average usage/impact** may be relevant factors in identifying candidate suitability and a purposive sample of financial services employees might still be achieved if the search could be advanced by searching for named individuals. Thus, the continuing methodology would next attempt a search for executive personnel from a small number of financial institutions. The social engineering framework (Mouton, Leenan and Venter, 2016) would be employed again in addition to the premise of suitable target, absent guardian and an organisation at risk of convergence. Instead of seeking personal contact details which 'The Corporate World' had proved impossible to obtain, the external assessment of risk would be disclosed to organisations as an incentive to participate in the research study. Chapter Five, 'Executive Risk' will continue the journey to data collection and illustrate how executive personnel may be a threat to their corporate employers.

Chapter Five: Executive Risk (Methodology Two)

5.1 Introduction

Executive Risk continues the chronological narrative documenting the methods used to obtain a sample for data collection. The first section (5.2) describes the construction of the research instrument to be completed by the recruited volunteers. Section 5.3 discusses preparation for the continuing investigation, including subjects to be sought and online resources to be used. The first 'exploratory' search is recorded to illustrate how the results shaped the parameters of the methodology. Section 5.4 provides a synthesis of thirteen challenging searches for executive employees documented in full in Appendix B. The successful search strategies are evaluated, and the thirteen searches are visually illustrated in Table 3 (5.4.4). Section 5.5 explains how findings from the practical research were used to incite interest from chief information security officers at selected financial organisations. Executive Risk concludes with the responses from the organisations and a reflection on how this may affect the sample for data collection (5.6).

5.2 The Research Instrument

The first draft of the self-completion questionnaire was developed in 2016, sixteen months before the survey was constructed using survey-building software. In the original format, forty-eight questions were divided into three categories relating to mobile device use, knowledge of technology and cyber awareness. Filter questions took applicable respondents to a short Internet of Things survey to ascertain employee engagement with consumer and lifestyle smart devices. The survey ended with a series of demographic questions.

In the interval between survey conception and production, consumer IoT devices evolved exponentially. To illustrate this in context, the original survey only expected to identify whether employees were bringing fitness trackers and smartwatches into the workplace. There were no questions relating to voice activated virtual assistants as Amazon Alexa launched in 2014 and had not yet reached mainstream acceptance (Mutchler, 2018). By the time the survey was constructed in February 2018, virtual assistants had become popular items alongside home systems for surveillance, security, music and other lifestyle requirements. The original questionnaire had been influenced by key themes seen in the literature but required updating during construction to reflect contemporary IoT security issues reported in the online media and technology press (see 3.11.4). Nonetheless, it had to be considered that not all users would engage with smart technologies. If the survey was augmented to include extra IoT-specific queries, stringent logic was required to ensure that avid consumers were examined in detail and users with no IoT were not alienated by questions of no relevance to their circumstances.

5.2.1 The Electronic Survey

The electronic survey took thirteen days to construct, using software provided by Smart Survey (https://www.smartsurvey.co.uk). A monthly business-standard subscription allowed access to key features including facility for complete anonymity. Respondents could be assured that identification was impossible as no IP addresses would be captured and only gender, nationality, and age was required as personal data. Skip logic would eliminate any questions not directly applicable to a respondent or their personal behaviours and the *user* was to be

the primary subject of the enquiry to encourage personal reflection. It was hoped that allowing respondents to focus on themselves would encourage completion, rather than an early exit due to boredom. To ensure inclusivity, questions would be directed at technically advanced users in addition to those with less competency or interest.

The first version of the completed survey was distributed to volunteers for pilot testing. Errors in the logic and piping entailed a further twenty-three revisions before all pathways operated correctly and piped answers created a bespoke experience for the respondent. The finished version contained seventy-two questions but regardless of the user's pathway, logic ensured that approximately thirty queries including six demographic questions were presented. Testers reported that the average time to completion was less than fifteen minutes.

5.3 A New Approach for the Practical Research

The narrative now returns to the research methods employed to recruit a data sample. ‘The Corporate World’ (Chapter Four) established that digital investigation aided by cyber-RAT had value for recognising average user employees in the context of **RQ1 actual/perceived risks** and **RQ2 average usage/impact** . Employee-generated social content suggested risk of targeted attack and identified potential candidates suitable for a purposive sample, but communication was not possible without using social media methods. A new approach would therefore circumvent the need to obtain personal email addresses but continue following the social engineering attack framework (Mouton, Leenan and Venter, 2016) whilst assessing exploitable data and user behaviour through the lens of cyber-specific RAT.

As discussed in 3.4.1, an average user may not realise now much information can be accessed via online sources (Hadnagy, 2010), nor appreciate the type of data an attacker might exploit (Junger, Montoya and Overink, 2016). Phishing typically employs semantic methods intended to instil a sense of urgency (see 3.4.2) and data extracted from social networking sites significantly improves the success of a phishing email (Jagati et al., 2007, p. 97). As targeted attacks are a regular occurrence (Symantec, 2017, p. 8; Symantec, 2019, p. 49), the online presence of high-ranking corporate employees would be explored to ascertain whether digital footprints might facilitate social engineering and position executive level staff as suitable targets. Large multi-national financial corporations may have already undergone bespoke CBEST resilience testing (BoE, 2020) (see 3.2) and it might be assumed that senior level financial personnel will have a greater awareness of the threat of cybercrime. Thus, if a sufficient number of senior executives and company directors could be theorised as an organisational risk, the anonymised results might be incentive for an organisation to take part .

5.3.1 Open Sources

Google Advanced Search to create search strings or search through domains and Google Images for reverse image searches are staple investigative tools alongside country-specific Google search engines. European data protection laws may prevent information being returned when searching for individuals and entering a search query into a Google engine based outside the EU can often produce results not obtained elsewhere. Google India, and Google Australia extend the reach of Google UK and are used extensively throughout the ensuing investigation. Additional open-source investigatory techniques make use of the Facebook Graph search feature. Graph allows advanced queries based on

Facebook posts and facilitates searching for photographs, ‘likes’, ‘check-ins’, groups and can connect profiles to find common themes between users.

Other resources would include people-specific search engines with enhanced performance, for example, Yasni (http://www.yasni.co.uk), Pipl (http://www.pipl.com) and Radaris (www.http://radaris.co.uk). These sites utilise public records and online platforms and search through multiple databases simultaneously to aggregate results. When used in conjunction with Google keyword searches, people-search engines can be very effective, although not guaranteed to return a ‘hit’ for every name used as a keyword. Online directories of public records are ‘deep web’ resources and cannot retrieve archived data using traditional search engines. Results are obtained using specific ‘dynamic’ searches (Bergman, 2001) and entering search terms into query fields. Online public records generally offer basic data for free and detailed information must be purchased. As an example, some address-finding resources will return a cluster of properties using the same postcode for free, but a specific address can only be obtained with a paid subscription. Examples of non-subscription public records used in the investigation included the UK Electoral Roll (http://www.192.com), British Phone Book (http://www.britishphonebook. com), and Endole Business Information (http://www.endole.co.uk).

5.3.2 The LinkedIn Account

Open-source investigation advocates anonymous browsing when using LinkedIn and ‘The Corporate World’ described how Google Advanced Search was used to find and view user profiles (see 4.9.1) until the LinkedIn website received an

upgrade. The ensuing modifications prevented a web browser from achieving direct access and LinkedIn profiles were subsequently viewed using language translation services to continue browsing anonymously. This method was employed again during ‘Executive Risk but ceased to function before the digital investigation was concluded. No other method to enable anonymity could be found so a LinkedIn account was created using the ‘Charlotte’ identity. Unlike other social networks which require an active email address to verify a new registration, LinkedIn demanded a valid telephone number. In professional open-source practice, a free Pay-As-You-Go mobile sim card is obtained and utilised for accounts requiring telephone validation. This elaborate process felt disproportionate for academic research and exceeded the use of a fake identity for safe-guarding purposes. The researcher was not comfortable using her own mobile number for a fabricated account and ‘Charlotte’ was deleted from LinkedIn as she could not be activated.

The investigation attempted to continue without LinkedIn, but the site is an essential open-source resource and social media accounts could not be verified as belonging to subjects without credible identification. Reverse image searches can only succeed if other images are available online (see 4.9.2) and without access to visual confirmation of identity, the investigations were impeded. To enable progress to resume, a heritage LinkedIn profile used for the researcher's professional practice was reactivated. This account had been created with a pseudonym for safeguarding purposes during an open-source commission for a private corporation and had maximum privacy controls activated. Users would be notified that their profile had been viewed, but as they could not access the

identity of the viewer it would deter them from attempting to make a connection with a pseudonym profile. The account remained active until the practical research was concluded.

5.3.3 Searching for Executives

'The Corporate World' described how one hundred and fifty-three (153) UK financial organisations were used as keyword searches (4.8.1). For the next methodology, the number of banking and insurance corporations would be limited to six. Organisations with a global presence and headquarters located in the financial centre of London were examined, and six corporations selected. The eminent financial institutions would be used as keywords to identify high-ranking personnel in senior positions. The next section (5.3.4) chronicles an exploratory search for a senior executive at an eminent organisation, this 'practice' search was key to developing the research methods and setting the parameters to be employed throughout the ensuing digital investigation. Images, text and current and archived digital content would be evaluated using cyber-RAT to ascertain suitable target in the context of **RQ1 actual/perceived risks** and **RQ2 average usage/impact**.

5.3.4 An Exploratory Search

The Boolean string "CEO" OR "Director" OR "Managing Director", and the name of one of the selected organisations was entered into Google UK and results contained the names of employees in senior global positions at the corporation. A search for online PDF documents returned current annual reports containing biographies of senior staff. For the exploratory exercise, the most senior individual in the corporation was selected as the subject. Entering the name as a

keyword returned ‘hits’ from online media resources, for example, Wikipedia, financial websites and financial industry press. Examination of these pages divulged place of birth, education, and the current geographical location of residence. The particulars were used for advanced searches, but the returned results were unavailable for public access and could not be viewed without purchasing a subscription to the news and industry websites holding the content. No social media accounts were returned using the keywords and open-source search techniques could find no further reference to the individual beyond that already retrieved. Despite considerable time devoted to the search it was not possible to locate personal information of value to an attacker and confirm suitable target. Subsequently, it could not be ascertained that the employees’ online presence was a potential security risk.

Open-source investigators acknowledge that there is always a valid explanation when data about a subject cannot be located (Smith, 2013; Smith, 2014). The exploratory search obtained no information of value, and it was concluded that an individual in such a high-profile position was likely to have protected their internet presence and operate under professional security advice to avoid potential online risks. An individual with responsibility to financial stakeholders would recognise their value to an attacker and presumably refrain from publishing personal content on social media. To avoid further time-wasting, the digital investigations required parameters to focus the search in a positive direction.

5.3.5 The Search Parameters

Data collection for a doctoral study must be achieved within a managed timescale and the failed methods undertaken during ‘The Corporate World’ left limited time

to complete the search for a sample. Thus, it was important to establish a framework to assist the investigation. A disadvantage of working with user-generated content is the time required to filter through substantial quantities of visual and text-based material to find relevant data. To combat this, each individual investigation would commence with a preliminary search lasting exactly thirty minutes. This would provide adequate opportunity to explore resources where data might be found and determine whether information about the employee was immediately available. If no appropriate data were returned by keyword and social media searches, another employee in a similar executive position would become the subject. If initial enquires returned results, the investigation would be allotted a further two hours to find sufficient information which the researcher in her role as theoretical social engineer might use for credible spear phishing. The total time was capped at two hours and thirty minutes to allow several searches to take place daily. In practice, if the preliminary search retrieved accessible data, the supposition of suitable target could be reached within one hour.

Should an exploratory search indicate that an employee shared a name with other active internet users such as celebrities, sportspeople or politicians, they would be replaced by another individual. This was to avoid the possibility of incorrect information being collected. Surnames perceived to be of foreign origin would also be excluded, as the preliminary search typically returned information in other languages. Despite the facility to translate text using the internet, accurate interpretation can not be guaranteed and poor translation may deliver incorrect information. It was additionally decided that less familiar surnames would be

advantageous, as opposed to very common ones. This would prevent the risk of confusing any individuals with duplicate names who might be employed by the same organisation. For example, there may be several Smiths or Collins in an office, but only one Weatherford. The intention was to locate individuals with an active web presence, and it was anticipated that many users would be found through keyword searches. It was crucial that a positive identification be obtained from a profile picture on either a social media account or corporate website. An individual without visual identification from more than one source could not be included in the search. Any personal data considered to be exploitable by an attacker would be temporarily recorded for the duration of the investigation in a simple text document. This would be stored on a password protected flash drive, retained in a secure environment, and accessed only by the researcher. All data would be anonymised, executives to be recorded only as job titles and family members documented as age and gender. At the conclusion of the digital investigation the document would be permanently deleted.

5.4 The Practical Investigation

Thirty-four financial executives were investigated following the search parameters outlined in 5.3.5. For fifteen individuals, the preliminary thirty-minute search did not justify an extended inquiry, but data retrieved about the other nineteen was sufficient to prompt further examination. Passive and active footprints (2.2.2 and 2.2.3) evaluated using cyber-RAT suggested that nineteen high-ranking executives may be suitable targets for spear phishing. In respect to **RQ1 actual /perceived risks,** user-generated content available on social media, combined with little or no controlled privacy may be an actual risk to corporate employers.

Appendix B chronologically documents thirteen of the nineteen searches; selected for potential interest to readers and other researchers. These challenging investigations used various search strategies, differing starting points, and required creative thinking (see 4.3.2) combined with open source tools and techniques (see 5.3.1). The six undocumented investigations were executed in the manner of the exploratory search described in 5.3.4 and personal data to assume suitable target was obtained within the allotted time of two hours and thirty minutes. The strategies used for the successful searches are synthesised into four key elements, used interchangeably throughout the practical research and the remainder of 5.4 provides examples from the digital investigation to highlight relevance to **RQ1 actual/perceived risk** and **RQ2 average usage/impact**. At the close of this section, Table 3 (5.4.4) will illustrate the thirteen searches and associated results. All searches referred to during 5.4 can be found in Appendix B.

5.4.1 Search Strategy: Photographs.

Staff biographies published to a company website are often accompanied by a professional photograph depicting the individual wearing business attire and posed in a corporate setting. Many users utilise their corporate photograph as a profile picture on LinkedIn and other social media profiles since the flattering image enhances the impression of financial executive, and the portrait is more aesthetic than a casual ‘selfie’ or amateur shot. When searching through multiple social media accounts held by users sharing the same name, corporate images as profile pictures enabled easy identification of pages belonging to a subject. Google Image searches for other online photographs often returned pictures taken at industry events, for example, conferences or trade fairs. Identifying a

subject in a picture containing many people was facilitated by recognising the business attire worn in the corporate image. Self-portraits or 'selfies' posted to a user's timeline validated identity and verified other social profiles. Comments left by other users in response to a 'selfie' customarily disclosed crucial data to be used for keyword searches or revealed accounts belonging to family or close acquaintances. In relation to **RQ1 actual/perceived risk,** digital images may be of value to an offender preparing a targeted attack. In respect to **RQ2 average usage/impact**, selfies are typically produced using a mobile device, thus, average usage may be contributing data adding to suitable target. An employee with publicly accessible and easily recognisable images on social media may be an actual risk to an organisation.

5.4.2 Search Strategy: Social Media

User-generated content on social networking sites, unprotected by privacy enhancing technologies and open to public view was used to corroborate data retrieved during keyword searches and prove identification of subjects or family members. To illustrate, Search 7 demonstrated how a media article briefly alluded to a particular sport and as a search term, the sport retrieved race results published to a club website. The subjects name was listed with a second individual sharing the surname and a search inside Facebook returned several profiles maintained by users with the surname. Individual inspection of each profile found accessible content relating to the sporting activity and identified the subjects eldest child. Other key data observed on the profile led to identifying the area of residence, school and eventually the residential address.

Occasionally, user-generated content provided the impetus to prevent a search from being abandoned. Search 9 was not making progress until an observation that the employee biography on LinkedIn referenced a past collaboration with charitable organisations and supplied relevant dates. Applying an operator to find PDF files accessed archived documents, and a report published in 2008 disclosed the spouse, stepchildren, and city of residence. The executive had (apparently) made effort to minimise self-published content and may have been confident of avoiding inappropriate monitoring. Thus, search 9 illustrates how passive footprints may subvert an average user's intention to maintain internet privacy. In respect to **RQ1 actual/perceived risks,** searches 7 and 9 demonstrate how passive and active data may be an actual risk to be considered by enterprise and risk managers.

5.4.3 Search Strategy: Recognised User Behaviour

Continual analysis of social network users eventually resulted in a (reasonably) accurate expectation of behaviours and an ability to predict those most likely to have a dynamic online presence according to their (self-assumed) aesthetic value. Individuals of both genders with particularly attractive features tended to be ardent social networkers with profiles on multiple platforms where content included many self-portraits and often exhibited a lack of activated privacy. The researcher realised that she may have been (unconsciously) selecting a subject if their photograph suggested a possible tendency towards social media narcissism (Bergman et al, 2011; Carpenter, 2012; Wang, 2017). Subsequently, Search 11 documents how a subject was deliberately selected for aesthetic appeal to ascertain whether attractiveness might equate to suitable target for a prospective

offender. In respect to **RQ1 actual/perceived risk,** a visually appealing employee with an active social media presence, or with capacity as an 'influencer' (see 4.7.3) may be a risk to an organisation. A 'narcissistic' user may have abundant unprotected personal data on several social media sites and may regularly maintain multiple profiles. Routine access from the workplace might expose a company issued device to malware and other nuisances (Ashford, 2019). Social networking may take place using mobile devices (3.9.5) therefore, regular access at work or in personal space using a device which connects to a corporate network has significance to **RQ2 average usage/impact**. Furthermore, attractive (narcissistic) users were observed to regularly post 'selfies' intended to incite responses from other users (Wang, 2017). Continuously accessing social media in the workplace to review user-responses using company property has relevance to **RQ1 actual/perceived risks.** Using a personal device to facilitate access is applicable to **RQ2 average usage/impact**.

Parent-executives with children were observed to habitually post content inviting feedback from others in their network. This included photographs of a child's birthday party, thus revealing a key date. Parent-users are very likely to have family members as social 'friends' and grandparents were regular commentators who responded to child and family-orientated content. Social media profiles of older users viewed during the investigation were generally not protected by privacy enhancing technologies (PET) such as privacy controls. Content and images lacking guardianship provided a steady source of information for key-word searching and established significant relationships. In addition, unprotected lists of 'friends' allowed access to other users profiles. In Search 8, a grandparent

posted photographs of the employee's children and other users contributed comments revealing the children's names. In respect to **RQ1 actual/perceived risks,** publicly accessible names and ages of children may contribute to an increased risk of targeted attack as a social engineer may misuse data of this type to prove credibility. Child-related data might be exploited to instil the sense of urgency required for a semantic attack to take place (see 5.3). Phishing emails containing malicious attachments continue to be a "proven attack channel'' (Symantec, 2017, p.38) and a parent may respond immediately if their child is named in the subject heading, particularly if the attacker has additionally obtained the name of the child's school (searches 3, 5, 7 and 13). A further consideration for **RQ1 actual/perceived risks** is that *images* copied from social media profiles may be misused in phishing emails. A photograph of children with their grandparent (see Search 8) might be sent to the subject in an email. A personal family photograph sent to a corporate email account would raise alarm or pique curiosity thus causing the instinctive reaction required to open a malicious email.

5.4.4 Search Strategy: Heritage Data

Archived material in national, local, or industry-specific media databases were a useful resource for search terms to be used in either Google UK or a Google engine outside the European Union. Articles and interviews can be retrieved using dynamic searches and modifying Google controls enables targeted examination of media resources for a specific time frame. Media content typically documented a subject's career path and provided keywords to access archived biographies from other corporate websites. Information included by a journalist to add human-interest, for example, sports (Search 7) or time spent in a foreign

office (Search 8) subsequently enabled directed searching. Interviews published in the generalist media (as opposed to industry-specific publications) often included familial details, including the spouse, number of children and occasionally a geographical area of residence. Search 13 demonstrates how heritage data identified social media profiles for a very senior financial executive, despite the user employing PET in the form of a pseudonym and not publishing any identifiable images. Average users may not consider heritage data as a risk to privacy and individuals with a varied career history and/or diverse interests might not realise where information is published or nor the type of data included in general-interest reporting. Passive footprints of this type are of value to open-source practitioners, but Rizzo (2016) cautioned that old data is of use for social engineering purposes. In regard to **RQ1 actual/perceived risks,** passive data may position an employee as suitable target for a directed spear-phishing attack.

Obtaining personal data for personnel at the very highest level proved to be a consistent challenge, and it was surmised that the most senior executives, usually with a global financial-media presence, make (apparent) effort to protect online identity and retain control over visible activity. Nevertheless, data gleaned from media and financial press archives generally facilitated a conclusive investigation. Average users may not recognise data of value to attackers nor where it may be found and in what quantity (Hadnagy, 2010; Junger, Montoya and Overink, 2016). The executives utilized as search subjects may not realise that regardless of minimal personal presence, content available elsewhere online places them at risk of convergence. As suitable targets they may become a passive or potentially active resource for an attacker (Hicks, 2018a) and in accordance with **RQ1**

actual/perceived risks may place their corporate employer at risk of victimisation. Table 3 (below) illustrates all thirteen searches and results.

Search	Starting Point	Search Strategy: Photographs	Search Strategy: Social Media	Search Strategy: User Behaviour	Search Strategy: Heritage Data	Results: Publicly Accessible Personal Data
1	Photograph (Corporate website)	Photographs on family profiles matched LinkIn profile.	1.Personal data on LinkedIn Profile. 2. Accessible social media content. 3. Family profiles revealed key data.	Older users without privacy controls.	Community newsletters, local area news archives.	Spouse. Parents & parents home address. Sibling. Community activities. Key friendships.
2	Photograph (Corporate website)	Social Media images matched corporate image.	Family profiles revealed key data	Parent-user posting images to invoke response.	European News Archives	Spouse. Home address. Business owner. Famous family member.
3	Photograph (Corporate website)	Social Media images matched corporate image.	1.Same username for all social media and online accounts. 2. Accessible social media content. 3. Family profiles revealed key data.	Parent-user posting images to invoke response.	Financial media articles. Archived staff biographies.	Spouse. Children. Home address. Childs school. Parents. Siblings.
4	Staff Biography (Corporate website)	Instagram account matched corporate image	1. Subject enabled privacy controls but was 'tagged' to friends accounts. 2. Friends profiles revealed key data.	N/A	N/A	Partner. Partners occupation & place of work. Key friendships.
5	Staff Biography (Corporate website)	Photographs on family profiles confirmed relationships.	1. Facebook domain linked people with same surname to specific geographical area. 2. Family profiles revealed key data.	Older users without privacy controls.	Financial media Articles. Archived staff biographies.	Spouse. Children. Childrens school. Home address. Parents. Siblings. Famous family member.
6	Executive Profile suggested by LinkedIn	Selfies' on social media matched image on LinkedIn profile.	1. Social media content identified family members. 2. Family profiles revealed key data.	Attractive User. Multiple profiles & 'Selfies'	N/A	Parents. Partner. Partners place of work, occupation & association with TV celebrities.
7	Executive Profile suggested by LinkedIn	1. Photographs on family profile provided key data. 2. Online photograph enabled identification.	Family profiles revealed key data.	N/A	Industry-specific & generalist news archives.	Spouse. Children. Childrens school. Home address. Club memberships and community actvities.
8	Keyword search in site: LinkedIn.com	1. Social media photograph matched those on corporate website. 2. Photograph with 'tagged' family members.	Social media content identified family members.	Older users without privacy controls.	Industry-specific & generalist news archives.	Spouse. Children. Childrens school. Parents. Address for two properties. Business Owner.
9	Keyword search in site: LinkedIn.com	Social media photographs matched LinkedIn profile.	Social media content identified family members.	N/A	Archived reports.	Spouse. Step-children. Siblings.
10	Keyword search in Google UK	Photographs in media articles confirmed identity.	Social media content identified family members.	N/A	Industry-specific news archives.	Parents & parents address. Siblings. Business owner. Key friendships. Voluntary activities.
11	Photograph Selected for user attractivenes	Photographs on websites identified area of residence.	1. Social media content identified family members. 2. Family profiles revealed key data.	Attractive User. Multiple profiles & 'Selfies.'	N/A	Child. Parents. Siblings. Extended family.
12	Photograph (Corporate website)	1. Instagram Photographs validated key relationships. 2. 'Tagged' family & friends lead to accessible accounts.	1. Subject 'tagged' to content in unprotected Instagram account. 2. Social media content identified family members.	Attractive User. Multiple profiles & 'Selfies'.	N/A	Parents. Key friendships.
13	Date-Specific Media Archives	Photographs of community events identified subject and spouse.	Family profiles revealed key data.	Older users without privacy controls.	Industry-specific & local news archives.	Spouse. Children. Home address. Both childrens schools. Parents. Siblings. Key friendships.

Table 3. The Search for Financial Executives

5.5. The Business Report

At the cessation of the digital investigation, nineteen high-ranking employees had been concluded as suitable target with potential risk of targeted engineering

attack. The anonymous findings were aggregated and compiled into a short business report produced for the attention of a busy professional. Key findings were highlighted in an executive summary, data was presented using graphs and charts to illustrate how employee use of social media was a potential risk and recommendations suggested improvements to social media policies. The report was not produced for the attention of academics or IT professionals but was to be sent to information security mangers who might share it with financial executives with limited knowledge of cyber security practices. Hence, the target audience was the average user of technology. The intention of the report was to entice corporations to participate in the project and provide volunteers to become respondents. It was assumed that if a security manager was interested, they may be obliged to take the discussion to the boardroom. Thus, all information contained in the report was clear and easily comprehensible so that decision-makers could appreciate the value in participating in the project.

To accompany the report, a one-page A4 document was produced specifically for the corporate chief information security officer (CISO). The document contained a brief synopsis of the research objective and explained that in order to theorise risk created by employee-owned technologies, data from financial sector workers was desirable. A request was made that members of the workforce volunteer to participate and to show appreciation, the anonymised aggregated findings would be shared. Findings may be of benefit for training purposes or to modify risk assessments to reflect contemporary lifestyle choices made by employees. The CISO was invited to email the researcher for more information and the university email address was included.

The paper documents were sent by post to officers based at corporate central headquarters in London. The challenge was to pique the interest of whoever opened the envelope and ensure that the documents reached the intended recipient without being rejected as junk mail. It was concluded that in the contemporary society of digital correspondence, a letter written by hand would be an oddity. To draw attention, a letter was written on quality writing paper to introduce the researcher and briefly allude to the risk to organisations created through employee use of social media. The recipient was encouraged to read the accompanying documents to illustrate why the organisation was being invited to participate in the research project.

5.5.1 Chief Information Security Officers

The recipients to receive the report were required to recognise that a project theorising unexpected risk to information security may be of value to an organisation. Furthermore, they needed seniority to take the project to stakeholders if they were interested in what they read in the documentation. Thus, the report was to be sent to chief officers responsible for global corporate security. To source appropriate individuals the string “chief information security officer” OR “Information security” OR “cyber risk” OR “cyber threat” AND “name of organisation” was used for all six corporations used in the practical research. LinkedIn profiles were evaluated to ensure the employee was a decision-maker with responsibility for practical security, including staff education, awareness, incident management training and risk assessments. It was important that cyber security managers were not selected as their responsibilities are generally IT specific and relate to digital networks and infrastructure. Cyber security

professionals may additionally conform to the viewpoint that technological systems need no assistance from the human element.

Open sources were used to find the postal address of the UK headquarters of the six financial organisations and the geographical location shown on the LinkedIn profile of each chief officer was located using Google Maps. This established whether the individual was based at company headquarters or at alternate premises. Six head office addresses and twenty people responsible for the security of corporate data were confirmed. The report, the project synopsis and the handwritten letter were placed in plain A4 envelopes. Although the hand-written letter was to pique curiosity, a hand-written envelope might be discarded as junk by whoever received and sorted the mail. Thus, first-class postage was bought from an online service and all address labels were printed to give a professional appearance and increase the possibility of the envelope reaching the intended recipient. The documents were posted in time for collection on Thursday morning in expectation of delivery on Friday. It was hoped that if the documents successfully reached the intended recipient, the weekend would provide opportunity for the CISO to reflect on the report and decide whether to act upon it or discard it. The twenty reports and documents were posted on 24 January 2018 and all data accumulated during the practical investigation was deleted from the USB flash drive.

5.5.2 The Outcome

In early February 2018, the CISO from one of the financial organisations emailed the researcher and asked to schedule a telephone conference. The conference

took place three weeks later and the CISO from this organisation (henceforth Bank A) was sufficiently interested in the project to offer help with access to volunteers. A soft copy of the research instrument and the hyperlink to the electronic survey was requested for review before it was forwarded to employees. In March 2018, the CISO from a second organisation (Bank B) sent an email to ask for a telephone conference. This took place in early April and the CISO showed great interest in the project, stating that it correlated well with current in-house research. The survey link was requested and sent immediately. Later in April, a third CISO sent an email stating that they would be unable to authorise potential volunteers but wished to assist by providing relevant data points. A telephone interview took place and the CISO discussed the security methods used in Bank C. No contact was initiated by the other three organisations, and it is unknown whether the report was received by the intended recipients.

5.5.3 Inadvertent Social Engineering

The handwritten letter sent to the CISO at each financial institution was meant with good intention to pique curiosity and prevent the accompanying documents from disposal as junk mail. The CISO from Bank B reported that when the documents arrived, the letter had caught the attention of the company secretary. She had then made special effort to deliver the report to him, rightly thinking he would be intrigued. The purpose of the letter was to ensure that the business report received attention and the CISO's comments confirmed that the method had succeeded. On reflection, this approach follows the framework of social engineering. The unsolicited letter was of interest to the CISO, and the content convinced him of credibility, to the extent that he established an email

correspondence. If equated to an attack scenario, this can be identified as reverse social engineering which takes place when a credible action convinces a target to initiate communication with an attacker. In a reverse attack, the target is the one who makes the initial approach and will, therefore, be more likely to 'trust' the assailant. If an attacker had been responsible for the letter which prompted the CISO to initiate email correspondence, malicious attachments masquerading as further documents may also have been accessed in the belief that they too were credible. Subsequently, the corporate network may have been threatened by the very person in charge of protecting it. This inadvertent social engineering highlights how susceptible humans may be when faced with apparent credibility. A copy of the report sent to financial organisations may be found in Appendix C.

5.6 Conclusion to Executive Risk

The search for executive personnel synthesised in 5.4 and documented fully in Appendix B provided substantive evidence that social media use may position a user as suitable target for targeted attack and is thus relevant to **RQ1 actual/perceived risk**. Content generated by the user or others in a network where guardianship is absent is also significant to **RQ1 actual/perceived risk**. If social networking takes place using personal devices, **RQ2 average usage/impact** also applies, not only in respect of routine device use to add to social media content, but regular access to social networks and the potential for convergence (see 3.4.3). Cyber-RAT and the theoretical fluidity between players suggests that a successful attack may place a senior employee as an instrument within the workplace and extend the reach of an offender (**RQ1 actual/perceived risk**). As a consequence, an organisation may become suitable target at risk of

convergence. The report sent to information security managers in 5.5 (see Appendix C for report) did not suggest cyber-RAT as a theoretical model and instead focused upon actual risk of accessible social media content as a gateway to targeted spear phishing (**RQ1 actual/perceived risk**). Three corporations responded to the findings and two offered assistance with access to volunteers.

The research methods applied in 'Executive Risk' achieved the desired outcome, the sample would be employees from the financial sector as dictated by the requirements of the study. Despite this, the social media user as an asset to academic research described in 'The Corporate World' (4.6.1) would no longer be present in the sample. Section 4.6.1 had anticipated that respondents would have an ardent, public social media presence and would-be active generators of online content presented for the approval and response of other users. In addition to **RQ1 actual/perceived risk,** such users would be an asset to social science research due to their ease with sharing personal values. Deviation from the methods in 'The Corporate World' due to the failure to achieve correspondent email addresses (see 4.10) entailed that instead of known social media users selected for the purpose, the sample would now be completely random. It may transpire that a significant number of the sample have little or no significant social media presence. These individuals may then be susceptible to "Question Threat" (Foddy, 2011, p.117) and either fail to complete the survey due to the questions causing discomfort or to pass over questions intended to acquire key data.

The exchange of a small but carefully curated purposive sample for a large random one may influence the quality of data collected by the research

instrument. Individuals selected by the researcher for their use of social media may be active users of personal devices, since ninety-nine percent of social media participants conduct activity using mobile devices (Statista, 2020b). Thus, data applicable to **RQ1 actual/perceived risk** and **RQ2 average usage/impact** would have been collected by the survey**.** Volunteers who participate in the study at the request of their employer but are not actively engaged in mobile social networking may not even bring a personal device to the workplace. The filter questions on the questionnaire may then lead a respondent on a pathway which fails to gather any data pertinent to the study. Without data relevant to device use in the workplace, the research questions cannot be satisfactorily resolved.

Nonetheless, an opposing, more positive perspective to the use of a larger, random sample may be predicted by evaluating the results of the practical investigation undertaken in 'Executive Risk'. Fifty-six percent of the executives displayed characteristics typical of the narcissistic social media user (Bergman et al, 2011; Carpenter, 2012; Wang, 2017) (see 4.6.1) and are consequently applicable to **RQ1 actual/perceived risk** and most likely **RQ2 average usage/impact.** If these findings are hypothetically extrapolated to accommodate a larger sample size, then it is possible that a considerable proportion of those surveyed will be active members of the online community. A larger sample has the potential to provide a superior quality of analytical data to answer the central research questions.

The offers of assistance from Banks A and B are where Chapter Five, 'Executive Risk' reaches conclusion. Chapter Six, 'A New Direction' continues the

chronological narrative documenting the journey to data collection, beginning in 6.1 with recapitulation of the outcome to ‘Executive Risk’ (section 5.5.2) to establish the reason for the methodology to continue into a third chapter. The introduction to Chapter Six begins at 6.1.1.

Chapter Six: A New Direction (Methodology Three)

6.1 Recapitulation of the Outcome of 'Executive Risk'

The report sent to each of the six financial corporations resulted in three CISO's expressing interest in the project (see 5.5.2). A series of conference calls took place with Banks A and B who both offered to assist the research and provide volunteers. Both banks requested the link to the survey and a soft copy of the research instrument for review before distribution to personnel. Bank C gave a telephone interview to provide datapoints. After the research instrument was sent to Banks A and B, the survey software was monitored daily, but no completed surveys were submitted. Despite concerted effort to re-establish communication, neither CISO would respond to emails. After two months, a final message was sent to Bank A asking for clarification. This evoked a response to confirm that the organisation was no longer able provide volunteers.

This disappointment compelled a renewed attempt to re-establish communication with Bank B and emails were sent to the CISO and his secretary. Initially, the researcher received no response, but eventually the CISO sent a message requesting another telephone conference which took several weeks to schedule as he was working abroad. The second discussion took place in late August 2018, four months after the initial offer of assistance. The CISO expressed continued interested in the project and asked for the research instrument and a brief project synopsis to be emailed to him. His intention was to forward the email to colleagues in the company and ask them to complete and share the survey. The survey link and synopsis were sent immediately, but no completed surveys

were collected. The CISO did not respond to any further communication, and it was finally concluded that Bank B would not be providing volunteers to participate.

6.1.1 Introduction to 'A New Direction'

Chapter Six will continue the chronological narrative and document the change in direction taken by the research methods after the financial corporations did not fulfil their offers of assistance. The final methodology is presented in two distinct segments. Segment 1, 'New Methods' commences at 6.2 and outlines how the researcher proposed to continue the digital investigation and complete the search for the purposive sample. Section 6.3 briefly summarises how the project was affected by new UK Data Protection legislation and directs the reader to Appendix D for a full description of the impact of the GDPR. Section 6.4 outlines the communication instruments used to invite respondents to participate and 6.5 defines the methods used to recruit the sample. At 6.6, Segment 2, 'Final Methods' records the additional efforts undertaken by the researcher, associates, and academic and industry colleagues to engage the financial sector in topical research of relevance to their industry. Section 6.7 evaluates the research instrument, addressing preparation of data for recording and analysis, errors in survey performance and manual data processing. Section 6.8 concludes the journey to data collection.

6.2 Segment 1. New Methods

Thus far the research methods had successfully theorised organisational risk and identified employees satisfying the requirements of **RQ1 actual/perceived risks** and **RQ2 average usage/impact**, but no primary data had been collected. A third change in direction was necessary for the final methodology and instead of

multinational organisations, local, independent companies would be approached. Derbyshire-based financial services providers, including mortgage and insurance advisors, financial planning agents and wealth management services were found using Boolean strings in Google UK. Organisations with a company website were selected for examination as those lacking an online presence in the form of a website or social media page were observed to be sole traders operating from a domestic residence.

The websites were perused for information about company personnel. Without exception, every organisation published biographies disclosing professional and personal information about members of staff, provided for the benefit of prospective customers. Some organisations introduced the senior professionals, others included a résumé for the entire team, including administration staff and apprentices, facilitating easy identification of directors and executive personnel. Section 5.4 illustrated how fragments of information can lead to key data, and personal details and images in employee biographies may be used to obtain social media accounts and other content available on the internet. For an attacker researching suitable targets, the company-generated data may easily facilitate social engineering. From the perspective of cyber-RAT, personal information available to casual observers suggests an absence of guardianship, places staff members in position of suitable target and may be an actual risk in accordance with **RQ1 actual/perceived risk**.

A personalised letter was to be sent to key personnel to invite them to participate in the project, and the staff biographies served as a useful indicator of

organisational hierarchy. In a business with multiple directors, the photograph positioned first in a list of personnel was always the director with overall management responsibility. Staff photographs exhibited side-by-side on the web page indicated a partnership or more than one founding director. In regard to **RQ1 actual/perceived risks**, these easily identifiable images of principal staff may place the individual in position of suitable target for directed attack, but for the purposes of the project the images identified potential respondents. Where it was evident that more than one principal members of staff had equal standing within the organisation, all principals were selected to receive a letter of invitation. Whenever it was not possible to discern the most senior personnel from data on the website, the UK government directory 'Companies House' was used to identify the primary director.

The initial search for financial services in Derbyshire took place in October 2018. Organisations varied in size and structure, ranging from partnerships with one secretarial assistant, to large enterprises consisting of a team of professionals and a range of staff in administrative and technical roles. Support staff were selected to receive letters of invitation according to their role within the company and likelihood that they would have authority to share the survey with other personnel. The job titles to receive invitations included Director, Managing Director, Managing Partner, COO, CEO, Head of Operations, Operations Director, Practice Manager, Office Manager, Technical Director and Compliance Manager. Postal addresses and any available email addresses were collected so that letters of invitation could be followed by an email reminder. Email addresses consisted of different formats, some staff profiles included a personal email address, other

organisations favoured a generic ‘enquiries@’ or ‘info@’ format. Some companies offered both a contact form alongside a generic email, others only the contact form. Larger organisations who favoured a contact form on their website, generally provided an email address on the company Facebook page. Of all the organisations selected, only two had no email address. At the cessation of the search for financial services in Derbyshire, contact details for sixty-seven (67) key members of staff in forty-five (45) companies had been collected. As these new methods deviated from those documented in Chapters Four and Five, it was now necessary to confirm whether ethical approval granted for the original research strategy was still valid before data collection continued.

6.3 The Change to UK Data Protection Law: GDPR 2018

Ethical approval granted in April 2017 by the University Research Ethics Committee had permitted digital investigation following the principles of the Data Protection Act 1998 (DPA 1998), the UK legislation in force at the time. The new methods described in section 6.2 not only deviated from those granted ethical approval, but the data protection legislation underpinning the research ethics was now obsolete. The General Data Protection Regulation (GDPR) had entered UK law on 25 May 2018, replacing Data Protection Directive 95/46/EC with a single set of robust data protection rules (GDPR, 2018). The change in legislation subsequently superseded the DPA (1998) with the Data Protection Act (2018). Had the project evolved according to the original research strategy, data collection would have ended before the GDPR came into effect. Instead, by the time it was conclusive that large financial corporations would not be involved, the GDPR was established in UK law and would affect any further effort to collect primary data.

The change to UK data protection legislation had considerable impact on the project, including a new application to the University Research Ethics Committee for ethical approval, restructure of the electronic survey and necessary modifications to the associated documentation to ensure compliance with the GDPR and the Data Protection Act (2018). The processes undertaken by the researcher to enable data collection to resume are documented in Appendix D.

6.4 The Letter of Invitation

When the second ethics application was approved, data collection recommenced, using the methods outlined in section 6.2. The GDPR compliant letter of invitation was printed in colour onto a University of Derby letterhead and began with a salutation using the recipients surname and the title Mr or Ms. The content was structured to convey key elements of the project and capture interest of busy readers. For brevity, bullet pointed sentences outlined the rationale of the research and benefits to the corporation if they were to participate. Although addressed to a named person, it was emphasised that all company personnel were invited to participate. The letter contained a simple, customised hyperlink which could be easily typed into an address bar or search engine to take the participant directly to the survey landing page. Recipients were invited to email the researcher or DoS for additional information or to ask any questions regarding the project.

First class postage was bought from an online service and the address label printed so that a professional appearance would avoid rejection as ‘junk’ mail. Scheduling was carefully considered, and letters were posted so that delivery

might avoid any anticipated busy periods where unsolicited mail might be discarded. As an example, the first cycle of letters was timed to arrive prior to the onset of the 2018 Christmas period to avoid being lost amongst increased volumes of festive post. It was hoped that having piqued interest, the letter would be retained for later review and a recipient might access the survey when time allowed. The letters sent in January 2019 were scheduled to arrive in the second week after the Christmas break, to avoid delivery when staff were catching up on work stockpiled over the festive season. The subsequent cycles were posted on Sunday night for early Monday collection and anticipated delivery mid-way through the week to avoid the busy period after a weekend. The letters posted to organisations located throughout Derbyshire generated the first completed surveys of the project. Following this success, financial services organisations were sought in other midland counties, including Nottinghamshire, Staffordshire, South Yorkshire, Cheshire and Leicestershire. A copy of the letter of invitation is available in Appendix E.

6.4.1 The 'follow-up' Email

Drawing on personal experience of small office environments, the researcher was aware that if an interesting item arrives when the recipients schedule is busy, it is likely to be put aside until a quieter time. To ensure that the letters were not put aside and forgotten, each one was supported by an email sent seven working days after the expected day of arrival. Each bespoke message was scheduled to arrive during a 'calm' period in a small office regime and would 'gently' remind about the invitation to participate in a PhD research project. To place this in context, recipients of letters posted in early December 2018 received email

reminders during the week when offices prepare to close for the Christmas break. It was anticipated that a reminder arriving in the lull before a holiday would entice employees to visit the survey if workloads were complete and time was available.

For the subsequent cycles, if letters were expected to be delivered on Wednesday, follow-up emails were scheduled to arrive a week later, during a quieter period where they might receive attention. Each email arrived mid-afternoon on Friday in anticipation that staff may have cleared workload ready for the weekend or have no further meetings scheduled. Emails were prepared in advance and stored in the 'drafts' folder of the researcher's university email account. All emails were then sent en masse, intended to arrive at approximately the same time.

6.4.1.1 Personal Email Addresses

An email reminder sent to a personal address opened with a salutation addressed to Mr or Ms and the appropriate surname. The brief content re-introduced the researcher and project and reminded the recipient that they had recently received a letter of invitation. The email referenced the name of the organisation and any colleagues who had also received letters. This was to offer reassurance that the email was not spam nor phishing and to encourage discussion between personnel who had been invited to participate. The email contained the hyperlink to the survey and the recipient was invited to share it with all colleagues. The message closed with thanks from the researcher and assurance that no further correspondence would be received and that email addresses would not be stored.

6.4.1.2 Generic Email Addresses

Emails sent to a generic email address including ‘info@’ or ‘enquiries@’ opened with ‘hello’ as salutation and immediately referenced the organisation and personnel who had received letters of invitation. As non-specific addresses are often monitored by administration staff, it was hoped that seeing familiar names might encourage continued perusal and prevent deletion as spam. No follow-up correspondence was sent to organisations who offered an enquiry form instead of an email address. It was deemed inappropriate to send a reminder for academic research using a form intended for customers to make legitimate enquiries. To comply with the assurance that email addresses would not be stored, all emails sent to organisations from the university account were deleted permanently from the server. It was noted that every time a cycle of reminders was sent, one or more of the respondents would email the researcher to report that they had completed the survey. This then caused the respondent to lose anonymity. Whenever these emails were received, a brief note of thanks was emailed in reply and all correspondence deleted.

6.5 Invitations

Between December 2018 and March 2019, three hundred and sixty-four (364) personal letters of invitation were posted to key personnel from two hundred and seventeen (217) financial organisations. The letters were followed by two hundred and fifty-two (252) email reminders. Small enterprises consisting of a managing director and one or more support staff typically received one letter addressed to the principal employee. Two principals in partnership each received a letter. Larger organisations tended to possess numerous key staff and

consequently each relevant person was invited. It was anticipated that offices receiving more than one letter might discuss the project and be motivated to participate. To illustrate with context, an organisation in Cheshire had seven directors based in the same office who were each responsible for a critical aspect of the business. Neither the company website, nor 'Companies House' made it clear which director had overall management responsibility, thus, invitations were sent to each director. Seven identical letters received from University of Derby may have initiated a conversation amongst directors and colleagues, and subsequently prompted participation. Table 4 (below) illustrates the quantity of letters and emails sent to organisations.

	Total Number
Individuals who received a personal letter	364
Organisations invited to participate	217
Organisations who received one letter	118
Organisations who received two letters	75
Organisations who received 3 or more letters	24
Email reminders sent	252
Individuals who received a personal letter and personal email reminder	136

Table 4. Invitations to Participate

6.5.1 Data Storage

As an incentive to encourage organisations to participate, the letter of invitation offered access to the aggregated findings at the conclusion of the PhD programme. This subsequently raised the issue of identifying which organisations had returned surveys, since no distinguishing data was captured. It was therefore decided that each of the invited organisations would be emailed a soft copy. As all project data followed best practice, the company names were saved to a

password protected pen drive and stored in accordance with the GDPR and the Data Protection Act (2018). Email addresses would be retrieved via corporate websites when results were ready for distribution.

6.6 Segment 2: Final Methods

Inviting employees individually had returned some completed surveys, but the project still lacked sufficient primary data for analysis and evaluation. Thus, the research methods had become an exercise in attempting to engage support from the financial sector. This final section of the methodology documents the approaches which took place concurrently with those described in Segment 1. The additional tactics were a necessary effort to obtain a sample of adequate size to complete the project. Segment 2: Final Methods concludes the primary data collection and 6.7 reviews the research instrument in preparation for the analysis in the ensuing chapters.

6.6.1 Profession and Industry Bodies

The financial sector holds five chartered societies and various institutes and trade associations to support businesses and individuals. These bodies set recognised standards, expect adherence to a code of conduct and offer accredited vocational education and opportunities for Continuing Professional Development (Business Dictionary, 2019). Membership offers extra value by granting access to a series of managed events including conferences, training courses and seminars. Many events are held abroad, and members are encouraged to network with peers. As the research methods had attempted to engage participation of bankers, accountants, insurers, financial planners and asset managers, the trade associations representing these individual professions were additionally sought.

Google UK returned websites for professional bodies which were examined to identify key personnel to receive the letter of invitation. The preferred choice was the chair of the management committee, the CEO or managing director, all assumed to have decision-making authority. Appropriate names and correspondence addresses were collected.

The format of the invitation letter was modified to retain essential GDPR requirements, research aims and objectives and the customised link to the survey. Additional content included a request that the survey link be shared with members or included on hard copy handouts and materials provided at future training events and seminars. The letter included an offer to supply further information if requested and emphasised that aggregated findings would be shared. Each of the chosen associations were advertising membership events to take place before the survey closed in May 2019, thus, the letters were posted in January 2019 to allow time for committees and boards to discuss the request and plan accordingly. Thirteen personally addressed letters were sent to principal staff and a copy sent to the head office of the organisation. The letters were not intended for any follow-up action as it was anticipated that if the request to share the link be authorised, the researcher would not be notified, unless a request was made for further information. Of the thirteen bodies approached, only one initiated correspondence via the email address included on the letter. The request to share the survey with members had been considered, but they were unable to offer assistance.

6.6.2 Financial Conferences and Training Events

Normative search methods using Google UK retrieved databases listing training events and conferences. These were perused for events aimed at generic financial sector professionals and not limited to those with membership of specific trade associations. Conferences addressing risk management for the financial sector, and emerging technologies in the financial services industry were selected for the direct relevance to the research. Each conference would take place in Europe or the UK before the survey was to close, and the researcher registered an interest in attending using the university email address. This granted access to individual event websites and open-source research techniques were used to find the name of the individual responsible for managing each conference. Nine bespoke GDPR compliant emails were drafted, outlining the project and associating the theme of each conference with the rationale and objective of the research. Each email included the survey link and was sent to the appropriate organisers asking if the survey could be shared with attendees or the link added to any materials to be distributed to delegates. These emails were not intended for any follow-up action as it would not be known whether the request had been successful unless an organiser asked for further information. As no additional completed surveys were received, it is assumed that the request to share the link was not approved.

6.6.3 Contacts

Professional and academic networks were approached and asked to assist by distributing the survey link to appropriate associates or by participating as respondents if associated with the financial sector.

6.6.3.1 Academic

University colleagues invited academic associates working in finance to participate in the research study. Representatives from two medium sized organisations in UK banking and four regional and international accountancy firms were informed about the rationale and objective of the project and invited to volunteer. Each request gained initial interest, but no organisation would commit to taking part despite an established working relationship with the academic who had personally issued the request.

6.6.3.2 Professional

Email correspondence was initiated (via academic introduction) with a senior employee at a multinational insurance corporation. The invitation to participate received positive response and a precis of the project was requested by the organisation. In December 2018, the researcher received an email informing that the invitation was being considered by stakeholders but cautioned that achieving full cooperation might take time. Throughout the first quarter of 2019, regular emails were sent to the organisation to request progress updates. A confirmation of participation was necessary to move forward as the survey was due to close 31 May. Emails were returned assuring that the employee was pursuing a response from senior managers. As no progress had been made by the final week of March, the researcher emailed the survey link to the employee and proposed that he share it with friends and associates in an unofficial capacity. This email went unanswered. In April, a mutual decision was taken to abandon the attempt to involve the organisation. The concluding correspondence advised that despite the initial positive response, approval from decision-makers could not be obtained.

6.6.3.3 Industry 1

A soft copy of the letter of invitation and the survey hyperlink were sent by email to a colleague from the risk management industry to be shared with financial professionals during cyber incident training. Delegates were to be informed about the research objective and encouraged to access the questionnaire. The colleague cautioned that he often observed during in-house training that financial employees struggle to find time to complete work obligations. Consequently, he anticipated difficulty in persuading delegates to submit an online survey.

6.6.3.4 Industry 2

An advertisement calling for financial professionals to participate in PhD research was posted in the Weekly Digest, an online newsletter available to members and subscribers of the Midlands Fraud Forum (MFF). The MFF is affiliated to the National Federation of Fraud Forums who work in conjunction with the private and public sectors in an effort to reduce fraud. Membership is wide-ranging, incorporating representatives from public bodies in addition to private sector organisations including banking and accountancy (Midlands Fraud Forum, 2014). The advert was a truncated version of the email sent to conference and event organisers and conveyed a brief project precis and the rationale for the research accentuated with bullet points to create visual impact. The advertisement appeared in the newsletter for four consecutive weeks between February and March 2019.

6.6.4 Personal Networks

Associates and friends with a personal or professional connection to the financial sector were sent the hyperlink and invited to complete a survey or forward the link to other associates in financial services. An acquaintance posted a request on social media, asking for all her Facebook friends who worked in finance to take the survey. A family member who works at Canary Wharf shared the link with financial colleagues employed in the area. Other family members working in local financial services were asked to complete the survey and share the link with friends and colleagues. An acquaintance with a close friend employed in information security at a high street bank enquired whether her friend's organisation might participate in the research. The request was turned down for fear of damage to brand reputation.

6.6.5 Regulatory Bodies.

A relationship was established with a senior manager at a financial regulatory body who shared the survey link with selected colleagues. She requested the questionnaire be completed as a personal favour and the link forwarded to others in their network with an appeal to participate as a gesture of goodwill. As a manager promoted to seniority from within the company, her colleagues were likely to be a combination of front-line team members, other senior personnel, and personal friends within the organisation. The survey was circulated on two separate occasions, a few days apart. Initial feedback from the senior manager indicated the survey had been sent to a few chosen colleagues who had shared it throughout their individual networks.

6.7 The Survey

The survey opened on 24 November 2018 and remained live for twenty-six weeks and six days, closing at midnight 31 May 2019 after collecting seventy-six submissions and twenty-eight partially completed responses (partials). A 'save and continue' option to leave the survey and later return to point of exit had been excluded, as users would have to supply an email address (Smart Survey, 2019), thus voiding the assurance of anonymity. Respondents were therefore obliged to complete and submit in a single session. Dates and times recorded by the survey software corresponded to cycles of letters of invitation and email reminders (6.4) and eighteen submissions and/or partials are known to have been generated following receipt of a written invitation to participate. Forty-four submissions and/or partials came from employees at the regulatory body, verified by date and time. The remainder were generated by personal contacts, professional and industry colleagues, trade associations, conference organisers and the advertisement posted to the MFF, but it is not possible to discern which method(s) achieved results.

6.7.1 Data Cleansing

Four of the seventy-six submissions were empty of data as participants were filtered directly to the departure page after stating they were not financial services employees. These were deleted. One completed survey was removed as the respondent worked in the finance department of a consumer goods manufacturer, outside the remit of financial services. Seven partial responses recorded between 16 and 23 November 2018 were deleted as they were known to be tests conducted whilst restructuring the survey to incorporate GDPR amendments (see

Appendix D). Twenty-one partials collected after 26 November 2018 were examined, as the date coincided with the first delivery of letters to the Derbyshire financial organisations. Nine recorded employment, type of mobile device and digital activity, but failed to inform whether personal technologies were brought into the workplace. Seven identified nothing beyond employment and personal mobile devices. These sixteen partials were deleted as they offered no data of relevance to the research questions.

Partially completed responses showing data in two or more sections were of interest as volunteers who had made effort to answer a considerable number of questions may have intended to submit but were unable to finish due to time restraints or interruption. Five partials provided sufficient data to contribute to the central investigation and were submitted as completed surveys. The total number of average-user financial services respondents who contributed data was seventy-six (N=76). Table 5 (below) illustrates the survey submissions, partial responses, and total number of respondents.

Submitted surveys recorded by survey software	76
Submitted surveys deleted for unsuitability	5
Total partial responses	28
Number of partial responses deleted from results	23
Number of partial responses added to results	5
Total Number of Respondents	**76**

Table 5: Survey Submissions

The sample size was disappointing considering the number of invitations and requests (see Table 4, 6.5 and section 6.6), but has the benefit of being entirely random, acquired from multiple services across the financial sector. If the offered

assistance of Banks A and B (see 5.5.2) had come to fruition, the sample may have been substantial, but employees would have been from two known organisations. Participants may have been selected by managers on account of compliance to organisational security or skill with technology and the element of 'average user' may have been lost. Generic company policies might have been reflected in the results and Silic and Back (2016) recognised the limitation of reliance on output from a data sample from a single enterprise. As a theoretic example, a ban on smartphones in the workplace may have resulted in very limited findings.

6.7.2 Restricted Questions

The four-part survey first examined personal mobile devices used for home and work based digital activities, then technological expertise and proficiency with mobile and internet-based technologies. A series of filter questions allowed appropriate respondents to access an Internet of Things survey and cyber awareness was followed by six demographic questions to conclude the questionnaire. In total, the questionnaire contained sixty-nine technology-related questions but with applied skip logic, each individual pathway featured approximately thirty queries. Compulsory questions had a restriction placed upon them to 'force' an answer to enable progression. These were predominantly filter questions to ensure specific criterion, or to direct the user's onward journey. Examples of criteria are the crucial requirement of financial employment to enable access to the questionnaire, and ownership of a mobile device without which a user had no value to the central investigation. Any volunteer not meeting these essential requirements was filtered from the survey.

Some enquiries were key to capturing data essential to the central investigation and would have benefitted from a restriction to 'force' a response, but it was deemed counter-productive to be overly restrictive. The survey contained so many questions that continually 'forcing' responses to allow progression may have hindered user engagement. A time-poor user may prefer to travel quickly through the questionnaire and forcibly impeded progress may have evoked survey abandonment. The disadvantage of permitting a faster journey was that some users opted to omit queries and several questions where key data may have been captured were occasionally 'skipped'. The dataset was not substantial to begin with and losing answers to critical questions may have impacted on the results. Nevertheless, technology users in contemporary society are accustomed to fast processing speeds, instant access and a speedy and seamless journey through cyberspace. Hence, it was preferable to achieve completed surveys by allowing fast and uninhibited progress instead of losing frustrated respondents halfway through the questionnaire.

6.7.3 The Summary Report

The survey was built using professional software, purchased for specific features including (amongst others) data protection, anonymity and design tools such as skip logic and piped answers. The in-built diagnostic resources were to assist with analysis and evaluation by providing a concise summary of results to identify key themes, and graphics to visually illustrate findings. A key requisite of the survey design was to maintain user interest so that respondents would not be daunted by the number of questions. Thus, to prevent irrelevant queries from

interrupting the survey experience, fifty-one pieces of tactically placed skip logic guided individual pathways and ensured that every question was applicable. When analysis began, it was noted that the summary report presenting the aggregated results contained segments where individual pathways could not be easily discerned. The confusion was caused by a key filter question primed with twenty-three pieces of logic. Figure 1(below) illustrates Participant Question Five (PQ5) copied from the online questionnaire.

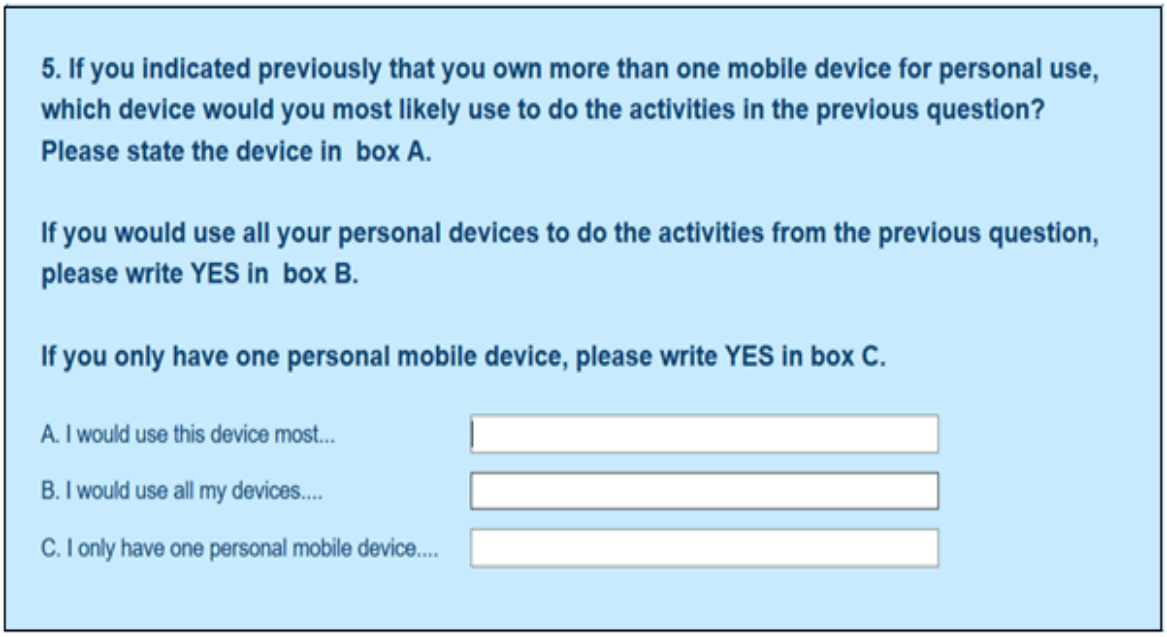

Figure 1. Filter Question PQ5

Respondents had already been questioned about mobile devices and personal internet activity and PQ5 shown in Figure1 (above) was to identify the primary device used for internet access and begin data collection for **RQ2 average usage/impact**. Owners of multiple devices were instructed to use Field A to classify the one habitually used for internet access. If all devices were used equally, the word 'YES' should be entered into Field B. Users who own a single device were to place 'YES' in field C. Multiple logic was built into Field A as the software was not sophisticated enough to recognise spelling alone nor accomplish

abstract reasoning. For example, a user might describe their device as a phone, mobile, mobile phone, iPhone, smartphone or smart phone. Text could be uppercase, lowercase or first letter capitalised. PQ5 would supply answers to be 'piped' into all into further questions to give personal relevance and also filter participants to appropriate locations in the survey. Thus, the logic had to anticipate how a user might respond to the question and incorporate the many available factors as operators. Figure 2 (below) is copied from a survey submission to illustrate logic and piping working correctly and demonstrate how responses to PQ5 personalise later enquiries.

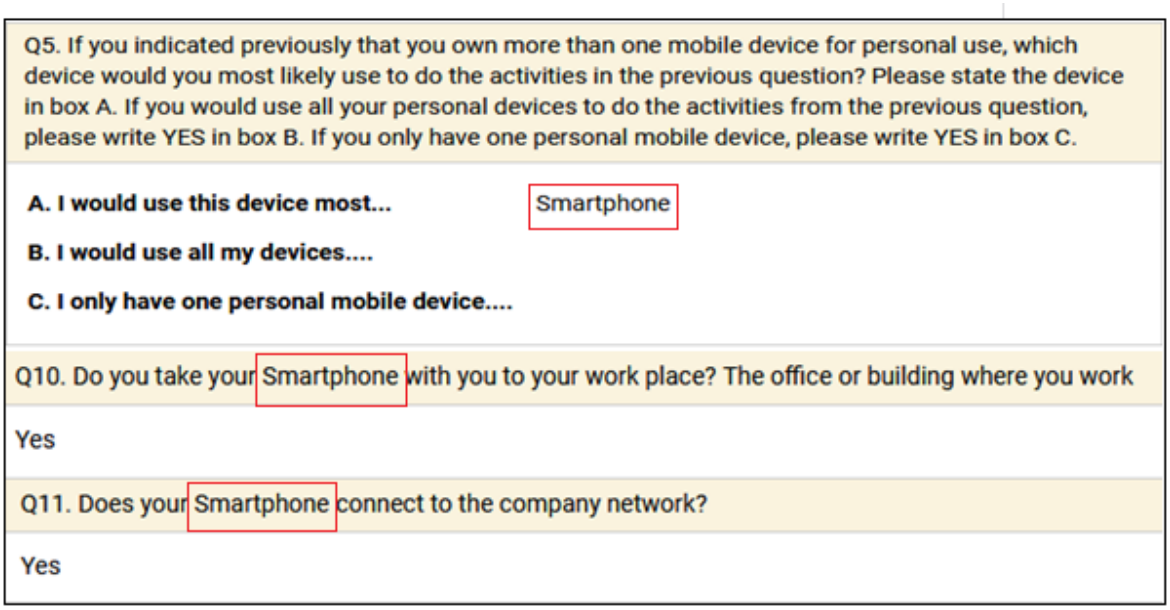

Figure 2. Logic and Piped Answers Operating Correctly

The logic in PQ5 performed as expected, but some respondents misunderstood or misinterpreted the question and caused errors in the aggregated results. PQ5 required only one answer field to be completed, but some participants placed answers in fields A, B and C according to the instructions. Each field was then recorded as a pathway in the results summary. Other users selected the answer

appropriate to their circumstance but placed it in the incorrect field, rendering the results summary inaccurate.

6.7.4 Mistakes in Logic and Piping

In addition to the respondent mistakes described in 6.7.3, an example of design error was identified in PQ5 where a word operator was inadvertently omitted from the skip logic. 'Phone', 'smartphone', 'iPhone' and other variants were included, but the term 'mobile' was overlooked. This affected the value of PQ6 and PQ7, key questions relevant to **RQ2 average usage/impact**. Figure 3 (below) is copied from a survey submission to illustrate the error.

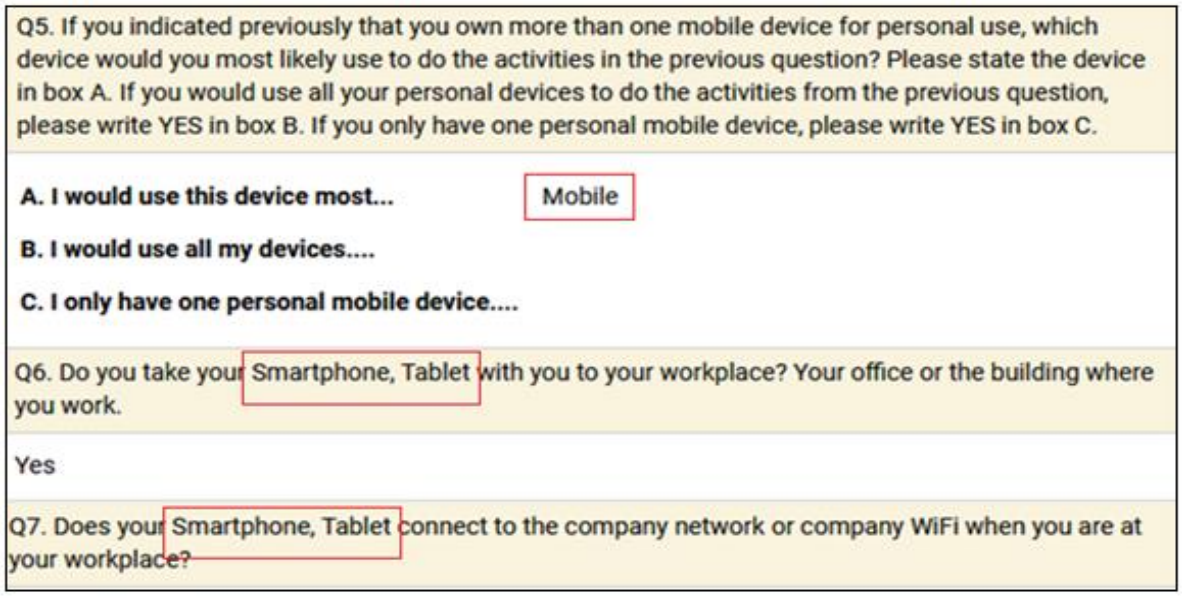

Figure 3. Mistakes in Logic and Piped Answers.

When answering PQ5 the respondent had correctly used Field A to state their primary device for internet activity, but the word 'mobile' had been overlooked as an operator to trigger logic. If 'mobile' been included, PQ6 and PQ7 would have referenced a single device and been explicitly clear that a mobile used for personal internet activity entered the workplace and connected to the corporate network, thus providing data for **RQ2 average usage/impact**. Without a correct

operator, PQ6 could only enquire about the two devices the respondent owned, rather than a targeted question using data confirmed by PQ5.

The design errors may have been due to the haste in submitting a second application for ethical approval leaving no opportunity for external testing to check for accuracy (See Appendix D). This was disappointing as the survey compliant with the DPA (1998) had undergone many trials until all flaws were resolved. Using a professional survey package instead of qualitative data analysis software such as NVIVO had been a deliberate decision, but it became obvious that the summary report did not accurately represent respondent activity. The graphics tools could not be used to create charts and tables as the exportable data was incorrect. Pathways relevant to internet activity and device use could only be seen clearly by visiting each individual survey submission and analysing the contents. Mistakes could then be corrected by examining answers to later queries and amending data accordingly. For example, Figure 3 (above) demonstrated that design error caused PQ6 and PQ7 to enquire about a smartphone and iPad, thus affecting the results summary. Examination of all data in the survey submission confirmed that a smartphone was the device taken to the workplace and connected to the corporate network, thus proving relevance to **RQ2 average usage/impact.**

As analysis progressed it became apparent that the diagnostic tools to aid in analysing datasets had limited capacity for qualitative interpretation. Results could be filtered quantitively, creating lists according to keywords or themes but listed items could not be accessed simultaneously. Datasets of shared traits and behaviours could not be compared against one another. To obtain qualitative

results, data was entered by hand onto paper wall charts. Manual data processing was laborious but allowed datasets to be viewed as a whole, enabling creative thinking (see 4.3.2) and identification of traits and trends in user behaviour (see.4.3.4). Data was then illustrated visually using charts and tables created by the researcher with Microsoft 365 Excel software.

6.8 Conclusion to 'A New Direction'

This third methodology chapter described the necessary change in direction after two large financial organisations withdrew from assisting the project before any primary data had been collected. Alternate methods were devised to continue using the internet as a tool to locate a sample of ideally suited respondents and new ethical approval was applied for and granted to ensure compliance with robust new data protection legislation. Digital investigation using only normative search techniques observed active data causing suitable target and in accordance with **RQ1 actual/perceived risks** implied that candidates appropriate for the purposive sample may be an actual risk to their corporate employers. Assorted methods issued two-hundred and twenty-six (226) financial organisations and twenty-two (22) professional and industry bodies with written and verbal invitations. Seventy-six (N=76) average-user respondents from a variety of financial occupations with a wide range of demographic representation completed detailed, bespoke questionnaires. Satisfactory data was obtained to evaluate personal technologies and digital activity in the context of suitable target and capable guardian and equate results with **RQ1 actual/perceived risks**, **RQ2 average usage/impact** and **RQ3 IoT unexplored risk**. Lack of engagement from financial personnel in conjunction with refusal of personally issued invitations

despite established working relationships suggested that financial corporations may recognise actual risk in the context of **RQ1 actual/perceived risks** and may wish to avoid addressing **RQ2 average usage/impact** and **RQ3 IoT unexplored risk**. This is evaluated later in Chapter 10. After addressing data cleansing and acknowledging errors and limitations in the survey design, Chapter Six, 'A New Direction' concluded primary data collection. The narrative will continue in Chapter Seven where the process of addressing the central investigation begins with recording the data in preparation for analysis and evaluation of the results.

Chapter Seven: Recording the Data and Content Analysis

7.1 Introduction

The complex research instrument provided considerable data, and the analysis, interpretation and subsequent discussion is substantive. This chapter (Chapter Seven) will begin by recording data to establish the context of the central investigation before introducing results relevant to the research questions. The chapter is structured as follows: Section 7.2 introduces the respondents and associated organisations and 7.3 establishes the framework of the study, commencing with personal devices and user interaction. Section 7.4 evaluates routine digital activity using expository data drawn from the literature to emphasise the requirement to examine mobile apps in the context of the corporate environment. In 7.5 the critical discussion relevant to the central investigation commences, beginning with apps installed to users' devices. Section 7.6 follows with an examination of personal device security and the chapter concludes in 7.7 Throughout Chapter Seven, findings with significance to **RQ1 actual/perceived risk** and **RQ2 average usage/impact** are visually illustrated with charts. This provides quantitative representation and is supplemented with descriptive interpretation and evaluation.

7.2 The Respondents

This next section introduces the sample to familiarise the reader with the respondents as ‘average users’ and will use charts, tables and descriptive text to illustrate data captured by the survey. Throughout the remainder of the thesis whenever a respondent is quoted or referenced, they will be referred to by the

number allocated by the survey software, for example, Respondent Number thirty-six or RN 36.

7.2.1 Age and Gender

Forty-one respondents identified as male and thirty as female. Five people chose not to provide gender data. Figure 4 (below) illustrates the total number of respondents in each age group.

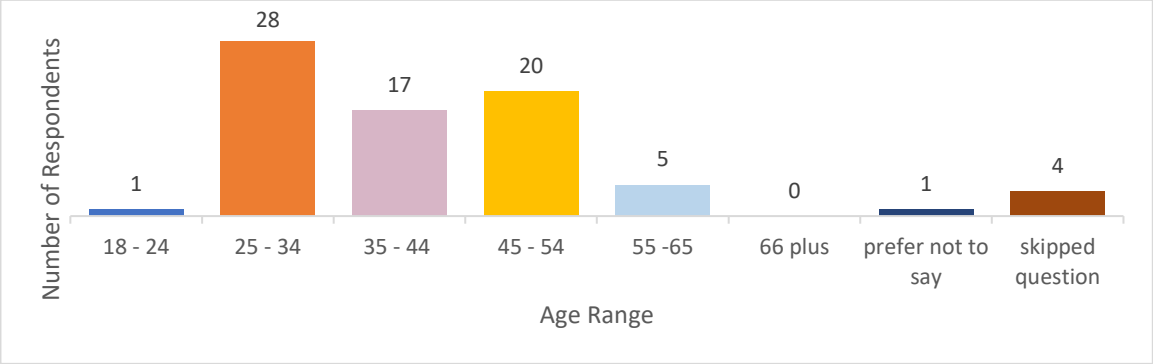

Figure 4. Respondent Age

Figure 5 (below) quantifies the ages and gender of the sample, demonstrating that the largest group came from the twenty-five to thirty-four demographic consisting of thirteen males and fifteen females. The second largest group were aged between forty-five and fifty-four and consisted of thirteen males and seven females.

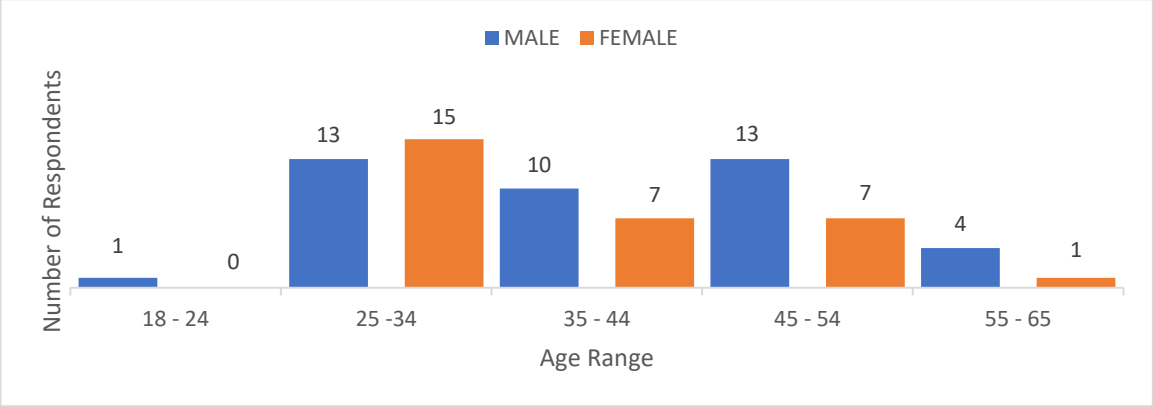

Figure 5. Age and Gender

7.2.2 Nationality

Respondents were invited to use free text to state their nationality. Figure 6 (below) illustrates results from seventy-one (N=71) respondents. Fifty-five participants identified as British, five as UK, five as English and two as White British. One respondent identified as UK with Pakistani origins. Only three other nationalities were recorded, Hungarian, German and Indian.

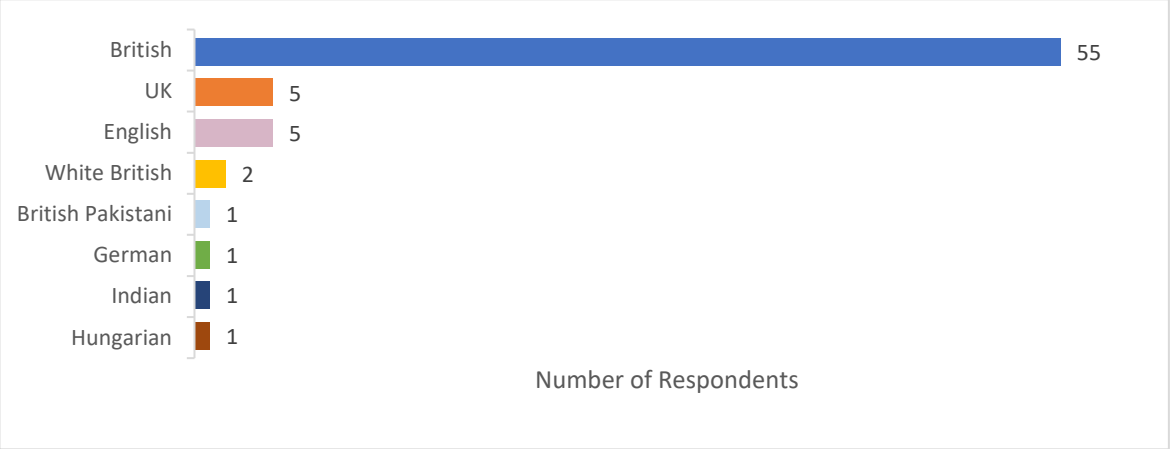

Figure 6. Nationality

7.2.3 Education

Respondents were invited to select their highest level of education, vocational or professional qualifications. A free text field was provided for additional comments.

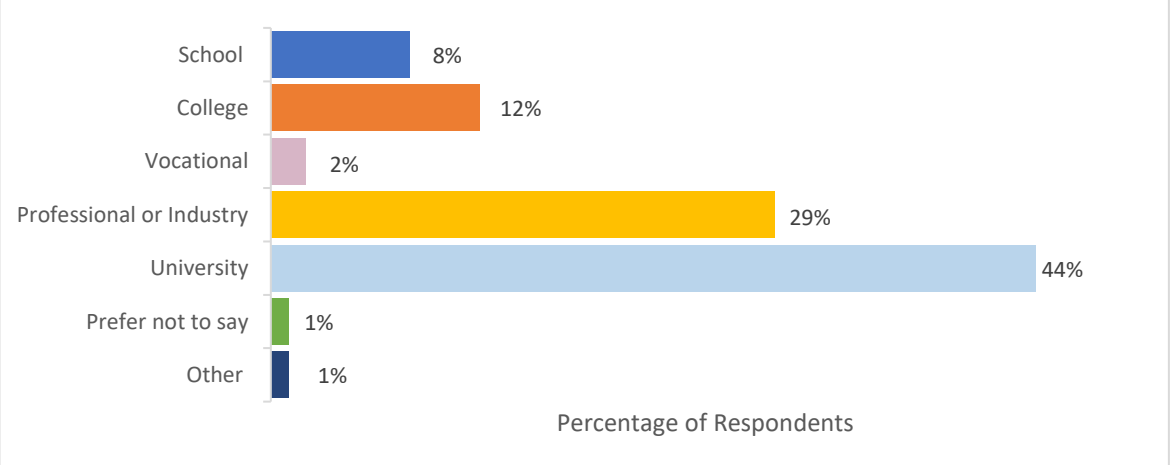

Figure 7. Education

Figure 7 (above) illustrates that forty-four percent are university educated and twenty-nine percent possess professional or industry qualifications. One respondent used the free text field to record their qualification as post-graduate Vocational Bar.

7.2.4 Employment

All seventy-six respondents are employed in UK-based financial services. The survey did not request geographical area, but it is known that organisations invited by letter are located in the Midlands and the regulatory service has branches in London and Coventry. Respondents were asked to categorise their financial service by choosing from a list of options. A free text field was available for additional comments. Table 6 (below) illustrates categories of service and number of employees from each one.

Type of Financial Service	Number of Respondents
Broker	1
Pensions and Investments	1
Forensics	1
Building Society	2
Insurance	2
Financial Services	3
Mortgage	4
Bank	5
Financial Planning / Advice	13
Regulatory Service	44

Table 6. Financial Services

Results in Table 6 (above) show that ten financial services are represented. It is unknown whether respondents from the same category of service are colleagues in the same office or from separate enterprises. Sixty-three (N=63) respondents used free text to clarify alternative financial services. These included thirteen from financial planning and advice, one broker, one pension and investment service, one financial forensics and three general financial services. Forty-four respondents stated that they were employed in regulatory services.

7.2.5 Participating Organisations

The total number of organisations could not be established from the results as no data to identify respondent nor corporation was collected. When filters were applied to the survey administration data, clusters were observed where a survey began and ended on the same date, in a narrow time frame. As an example, Table 7 (below) shows filtered results copied from the survey software.

18	18/02/2019 12:38:32	18/02/2019 13:45:18
19	22/02/2019 11:21:12	22/02/2019 11:32:59
20	22/02/2019 14:49:50	22/02/2019 15:05:10
21	22/02/2019 14:50:35	22/02/2019 15:07:16
22	22/02/2019 14:52:43	22/02/2019 15:04:52
23	05/03/2019 06:22:03	05/03/2019 06:37:05

Table 7. Dates and Times of Survey Completion

The highlighted data in Table 7 illustrates how three surveys were started and submitted in a single twenty-minute time frame on Friday 22 February 2019. This is consistent with the methods described in 6.4.1 detailing how the email reminder was timed to coincide with an assumed quiet period in the office environment. The three respondents illustrated in Table 7 used free text to describe their

organisation as a ‘financial advice service’ and their occupation as executive or senior. They might therefore be assumed to be colleagues in the same company. Using this method to evaluate data clusters implies that twenty-seven organisations took part, although these results can only be speculative. The actual number of participating organisations has no bearing on the results since the employees were the primary dataset. Nonetheless, considering that two hundred and twenty-five (225) organisations were personally invited to take part, a twelve percent participation rate is of interest. The reluctance to be involved in research investigating a topical issue of direct relevance to the financial sector is reviewed in section 10.3.

7.2.6 Occupation

Participants were asked to choose the option which best described their position in the company. The choices of ‘executive’, ‘senior manager’, ‘middle manager’, ‘manager/supervisor’ and ‘clerk /officer/associate/ admin/ frontline staff’ represent the hierarchy of a corporate office. Figure 8 (below) illustrates the results from a sample of seventy (N=70).

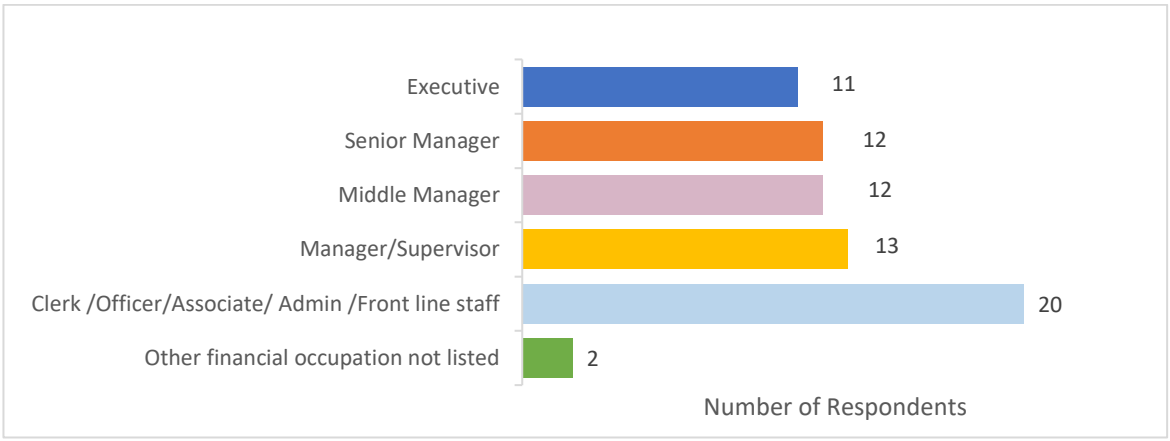

Figure 8. Occupation

7.3 Personal Technologies

The results for 7.3 are presented following the sequence of questions on the research instrument. This format will establish the behaviours of the sample and begin the discussion surrounding personal technologies and user interaction. The research instrument did not invite respondents to declare make, model or favoured operating system since this data had no relevance to the results. The objective was to discover how users interact with their technologies and not discern the popularity of specific devices. For reference, a 'smartphone' is a mobile telephone with internet connection and a digital operating system.

7.3.1 Personal Mobile Devices

Participant Question three (PQ3) invited respondents to indicate any mobile devices owned for personal use. The options were 'smartphone', 'tablet' or 'iPad' and a free text field was provided to add any device not in the list. Results illustrated in Figure 9 (below) show that that one hundred percent of respondents own a personal smartphone.

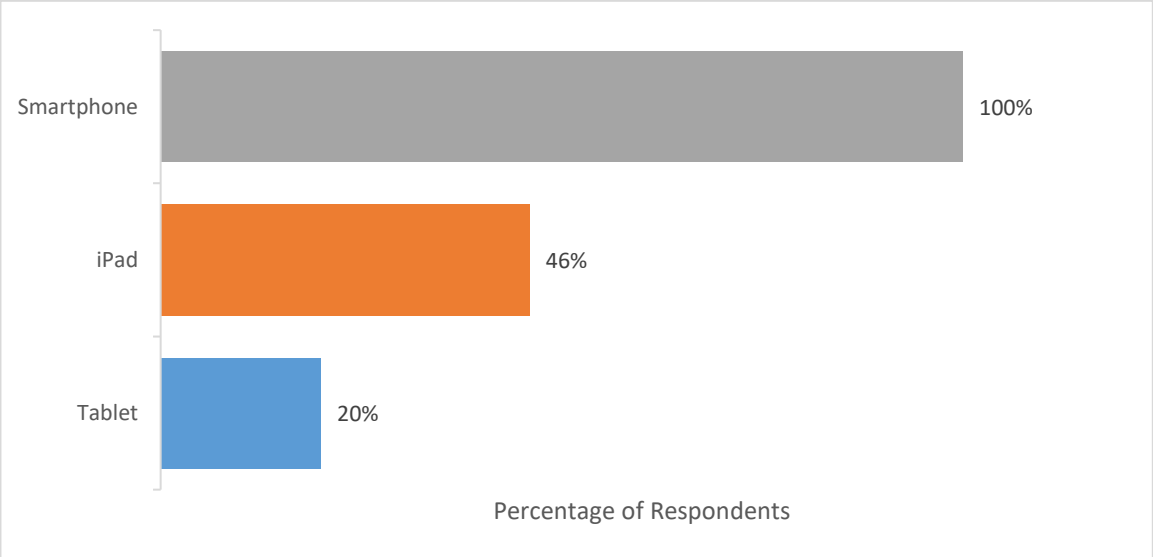

Figure 9. Personal Mobile Devices

Despite no instruction to describe their device, thirty-one respondents used free text options throughout the survey to specify their smartphone as an *iPhone*. This suggests that Apple users differentiate iOS from other operating systems. Therefore, if the term 'tablet' had acted as an all-encompassing descriptor to include iPads, tablets and other large-screen handheld devices, those who distinguish iPads from tablets may not have responded. Placing tablets and iPads into separate categories may have increased the response rate for PQ3. In addition to identifying ownership, PQ3 measured the number of devices possessed by each participant. Thirty-nine percent of respondents own a smartphone and no other devices. Forty-one percent own an iPad and smartphone, fourteen percent own a tablet and smartphone, and five percent own three mobile devices. These results are illustrated by Figure 10 (below).

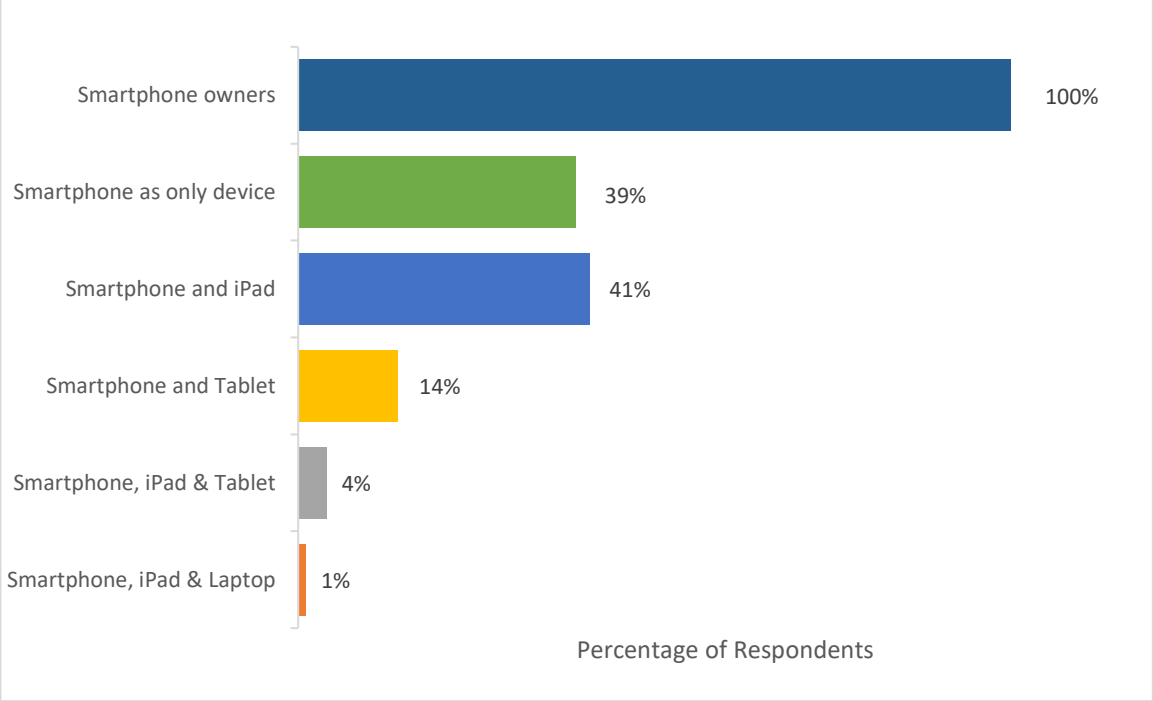

Figure 10. Quantity of Owned Personal Devices

7.3.2 Personal Internet Activity

PQ4 offered a choice of fourteen internet activities and respondents indicated those undertaken using personal devices. A free text field was provided to include any additional activities. One hundred percent of respondents contributed data to PQ4 with seven respondents adding extra activities. Use of communication apps including WhatsApp, Messenger and Snapchat was the most popular activity, affirmed by ninety-six percent. The lowest percentage applied to users visiting online casinos, but this result may be limited by incorrect terminology and reference to casinos instead of *gambling*. A more definitive set of data may have been produced if the enquiry had asked about online games to win money. Figure 11 (below) illustrates the most popular activities and indicates those with lesser, yet still significant response rates.

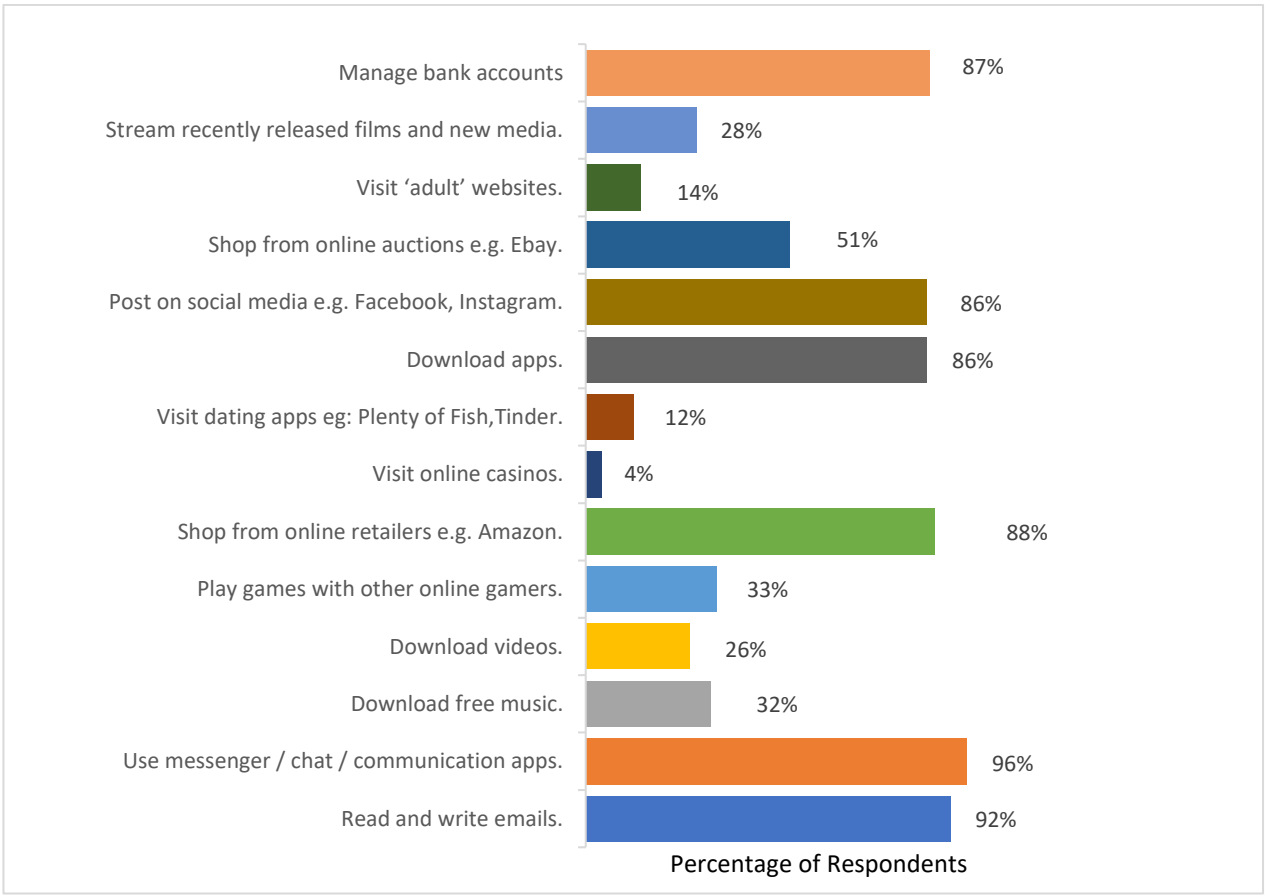

Figure 11. Personal Internet Activity

7.3.3 Mobile Devices and Internet Activity

Having ascertained the personal internet activity undertaken by average users, PQ5 queried the devices used to conduct the activity. Three options were provided to indicate the principal device, demonstrate that all devices were used, or verify possession of only one device used for all internet activity. Seventy-one percent confirmed a smartphone as the primary device for internet activity, twenty-five percent use all devices and four percent use an iPad. Sixty-five (N=65) people provided data. Figure 12 (below) illustrates the percentage of respondents and the devices used for internet activity.

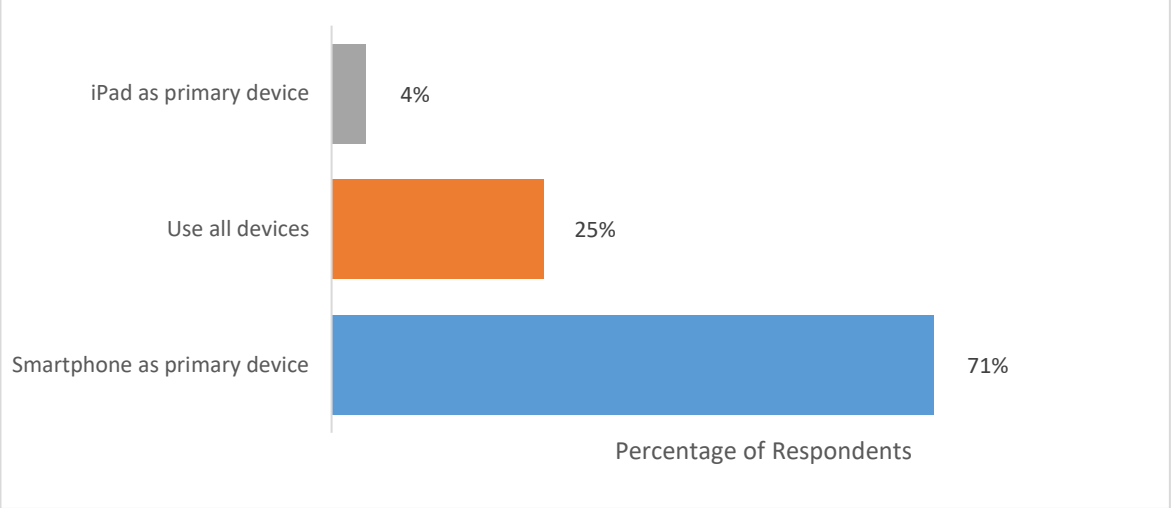

Figure 12. Primary Device used for Internet Activity

7.3.4 Mobile Devices in the Workplace

Seventy-five (N=75) respondents confirmed taking a smartphone to the financial workplace and thirty (N=30) take more than one device. Of the sixteen respondents who use all devices for internet activity, thirteen (N=13) confirmed that all devices accompany them to work. Only one respondent claimed to take no device to the workplace. Figure 13 (below) illustrates the number of respondents and the type and quantity of devices brought into enterprise space.

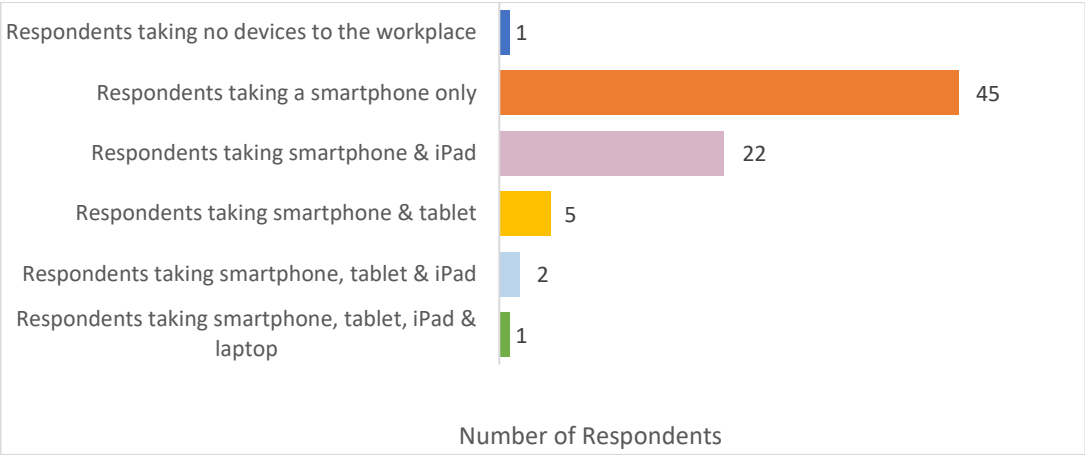

Figure 13. Type of Devices Taken to the Workplace

The total number of devices brought into the financial workplace by seventy-six (N=76) respondents totalled one hundred and nine (109). Figure 14 (below) illustrates three results: quantity of smartphones, number of users carrying two or more devices and the total amount of devices present in the financial workplace.

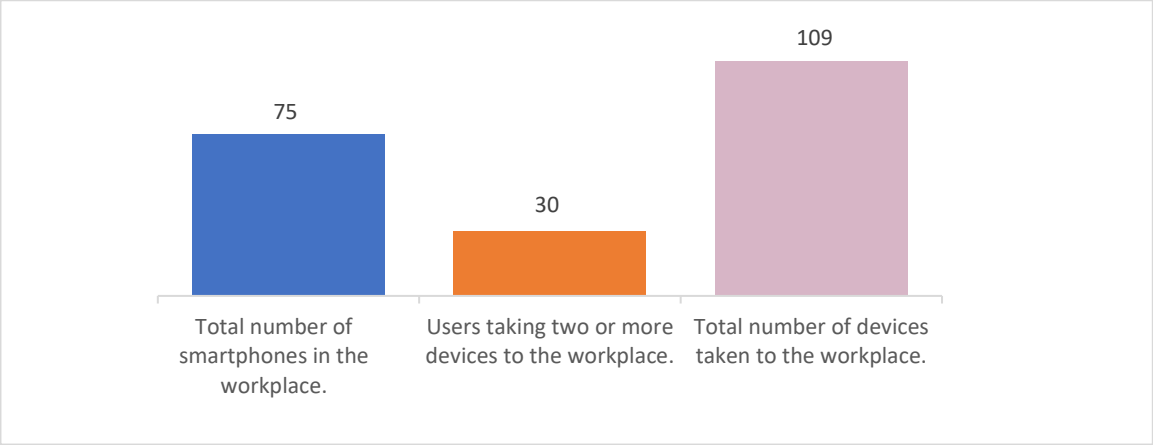

Figure 14. Quantity of Devices in the Workplace

7.3.5 Work Activity using Personal Mobile Device

Fifty percent of respondents passed the question regarding work activity using personal devices. Figure 15 (below) illustrates a sample of thirty-eight (N=38).

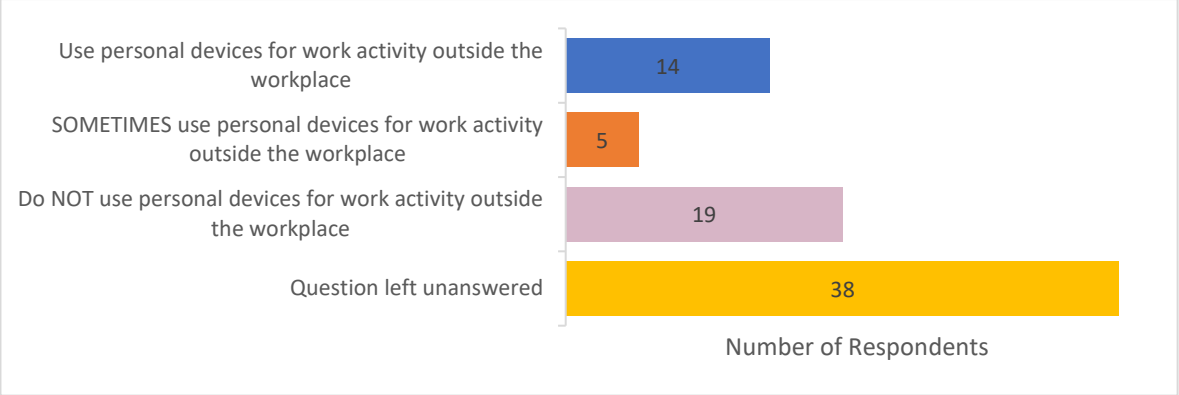

Figure 15. Devices used for Work Activity

Figure 15 (above) illustrates that fourteen participants do use personal devices for work purposes, and five use them sometimes. Free text was used to describe the type of activity and included emails, reading articles, watching YouTube, calendars and remote access when home working. Nineteen participants stated that their devices were not used for work purposes. Skip logic functioned correctly during this section of the survey, hence, the fifty percent who passed on the question may be the first indication of "question threat" as suggested by Foddy (2011, p. 117). Those who use their devices for unauthorised work activity may have found the question uncomfortable. Further discussion of unanswered questions may be found at 9.2.3.

7.4 A Brief Evaluation of Routine Activity using Mobile Apps

The use of applications is a fundamental element of mobile technology and allows devices to be used for practical operations such as navigation and language translation, or entertainment by providing access to music, media, news or sports. Services are accessed by downloading a designated piece of software to enable specific tasks (GCF Global, 2019). Google Play and the iOS app store are the two largest distributors, although more than four hundred providers are in operation (Natanson, 2019). Apps are available for numerous services including

some that serve no purpose other than to amuse (Khabar, 2018). So that the significance of apps and personal devices in relation to the cyber-RAT framework and the central research questions can be appreciated, Figure 16 (below) quantifies respondent use of app-based internet activities indicated by the literature as those with capacity to introduce harm. In the context of cyber-RAT, these activities may place the user in position of suitable target, at risk of convergence with an offender, or instrument extending reach of an offender and are relevant to **RQ2 average usage/impact**.

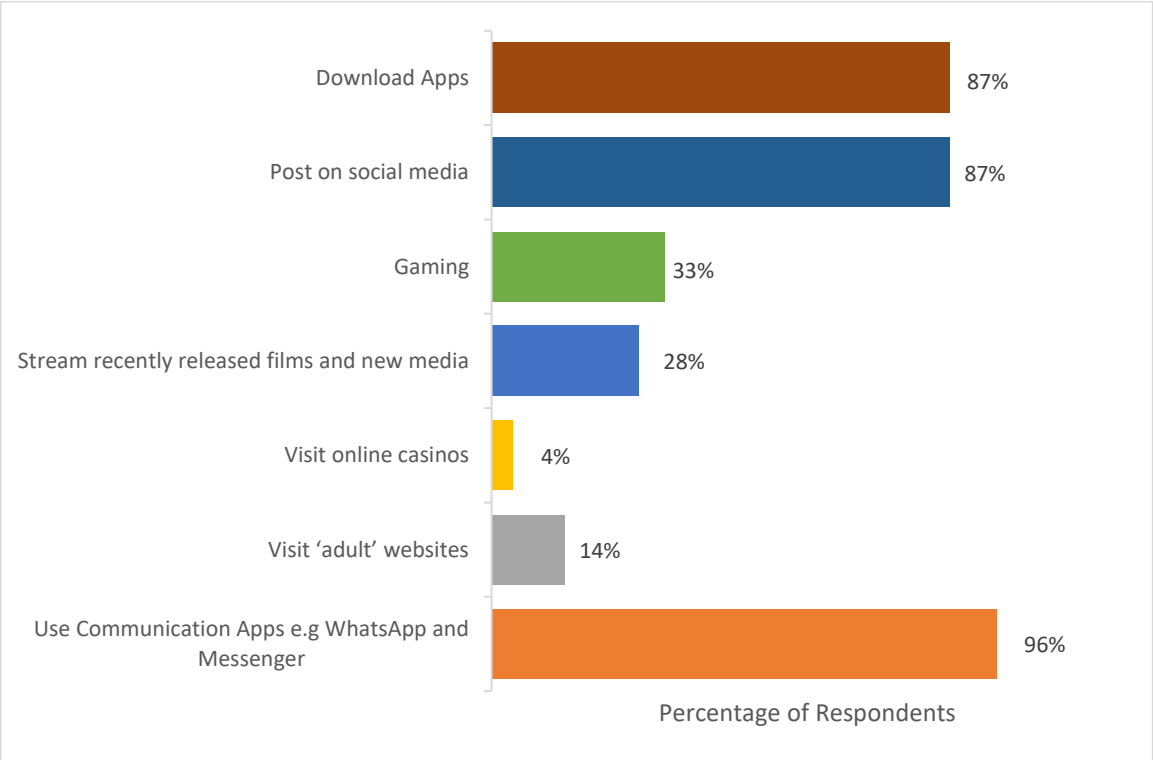

Figure 16 Routine Activity using Applications

Eighty-seven percent of respondents confirmed routinely downloading applications. Section 3.7.3 established that malware in disguise is a valid threat and high-risk apps may be found on mobile devices (McAfee, 2019; Symantec, 2019). Lifestyle, tools and entertainment apps are the categories most often seen as malicious (Symantec, 2019) and Figure 16 (above) illustrates routine access of

entertainment apps proving access to streaming, gaming, dating and adult content. Thus, in regard to **RQ2 average usage/impact,** entertainment and lifestyle apps are present on devices brought to the workplace. Although no data was captured regarding use of *specific* apps, utility tools such as note-taking or content management apps may have value to office-based employees and digital sticky notes, mind mappers or password managers (Guay, 2018) may also be installed to devices.

The literature emphasised that software cannot be developed without the presence of errors or flaws (Kaspersky, 2016; Reis, Barth and Pizano, 2009; Zhang, Raghunathan and Jha, 2014) and the more code operating on a digital system, the higher the probability that a security vulnerability may be present (Rouse and Haughn, 2019). To place this in context, the more apps on a smartphone, the greater the possibility of an exploitable flaw. The remainder of 7.4 will provide a succinct evaluation of threats made possible by applications, recognised by academics and the security sector. Risk of harm is increased if a vulnerability is unknown to the developers and no repair has been issued. If the vulnerability is acknowledged and a patch to resolve the flaw has been produced, then any user who does not install the update-as-guardian remains vulnerable to a risk of convergence.

7.4.1 Streaming

One of the major growth areas of the app economy is entertainment (Sydow, 2018) and industry experts estimate that by 2021 users will spend one hundred minutes streaming video every day (Chaffey, 2020). Over half the video content

streamed by users is viewed on mobile devices (Lister, 2020) and includes short video like YouTube, social networks where video is included as content and ‘on demand’ subscription services. Streaming, where video data is delivered continuously via the internet (Techopedia, 2019) has resulted in the creation of over one hundred service providers (Cook, 2019). Access to popular content can require subscription to many services and the cost of viewing can become “prohibitively expensive” (Bode, 2018, para. 11). In addition, original content exclusive to an American provider may have poor international distribution (Cullen, 2018, para. 2) or restricted geographical viewing (Bode, 2018, para. 11). Legitimate subscribers may desire access to content unavailable on their services (Chatterly, 2019, quoted in Stokel-Walker, 2019, para. 11). Subsequently, users may pay for one or two selected services and any other content they wish to view is accessed illegally by using services to supply ‘free’ pirated content (Cullen, 2018, para. 2).

Users may not equate piracy with theft as digital content has no physical presence (Putman, 2019), and users may consider it to be nothing more than accessing something for free. For some, deliberate, self-interested lawbreaking is motivation (Breakey, 2018) as content should be freely available and users are not willing to pay for it (Putman, 2019). Some streaming service content may be downloaded for offline viewing but typically expires after a limited time, therefore “having permanent copies of things appeals to me” (Alister, 2018, para. 7). This suggests that indefinite storage of pirated material may also be incentive for illegal access.

7.4.2 The Significance of Access to Copyright Protected Material

Average users wishing to access free media can conduct a simple Google search and find instruction on how to stream or download without payment, but copyright protected 'pirated' media content is commonly exploited by attackers (Batt, 2019; Daryabar et al., 2016; Fan, 2015; Paganini, 2019). Criminals pay providers of illegally obtained content to place their malware where it will be encountered by users seeking to download material (Fact, 2017). The free download arriving to the users' device may look like the content ordered, but when opened, malware will be activated (ibid, 2017). Threats including backdoor trojans and other unwanted software can be accessed alongside the content (EUIPO, 2018).

More recently, popular television shows attract viewers willing to access copyright protected content before the official release date. An example is the fantasy drama Game of Thrones. If the premiere of each season were not scheduled for simultaneous global broadcast, an illegal copy would be accessed the moment it became available (Cullen, 2018). Security researchers found thirty-three different threats infecting illegal downloads of the first and last episodes of every season (Kaspersky, 2019a). The first episode of the final series was pirated fifty-four million times (54,000,000) in the first twenty-four hours after the official premiere (Cuthbertson, 2019a). In the context of cyber-RAT, users who access copyright protected content position themselves as suitable target. For the malware distributors, every download is a convergence with a suitable-target digital system. In the absence of the user-guardian, capable guardianship must come from a well-secured device.

Twenty-eight percent of respondents confirmed that they stream video and new media. The survey did not specifically ask respondents whether they accessed copyright protected material, therefore results may or may not reflect use of legitimate streaming services. This is debated further in the discussion and can be found at 9.3.4. To clarify, the concern to organisations is not the illegal access of content, but the risk of encountering malware which may compromise a device and subsequently a network. Evidence that streaming takes place using devices brought into the workplace is relevant to **RQ2 average usage/impact.**

7.4.3 Games

A second area of the app economy experiencing major growth is gaming (Sydow, 2018). Approximately fifty percent of those who engage with mobile apps are games players and thirty-three percent of app downloads in 2019 were for mobile games (Kaplan, 2019). UK mobile gamers are assumed to number over nineteen million (19,000,000) with thirty-nine percent of users in the twenty-five to thirty-four age group (Statista, 2020d). Seventeen percent of gamers are thought to play games from the moment they wake in the morning, with ten percent playing at school, university or in the workplace (Deloitte, 2019). Some smartphones are specifically designed to enhance the gaming experience. These include features such as a large antenna to prevent loss of signal when the gamer wraps their fingers around the device and a liquid cooling system so that intense gaming will not cause overheating (Lumb, 2019).

7.4.4 Games Malware.

Quality games are not free. Consequently, the market for free games apps is enticing players to disregard due diligence and popular games are used to entice users to download malware or other scams (Sullivan, 2018, quoted in Hern, 2018b). A user may download 'game cracking apps' to modify games and grant access to premium features without payment (Boricha, 2021), allowing players to "score more and level up quicky" (Boricha, 2021, para. 3). A 'cracked' game has been modified so that users can play without paying (Jefferson, 2021), by removing the Digital Rights Management (DRM) licence which prevents the game form being copied and distributed (Chaudhry, 2017b). Cracking the game entails that either the code is altered, the safety features are 'tricked' or the system which should check for certification is disabled and users gain free access to all the resources such as "coins, gold, ranks, unlocks" (Boricha, 2021, para. 6). A simple search using Google can find many third-party app stores providing free versions of 'cracked' games, and websites and fora providing lists of recommended 'cracking apps'.

As pirated games are attractive to gamers, they are common vectors for malware distribution. Attackers use public places on the internet such as Facebook events calendar and Google Groups to advertise links to a site where cracked games can be obtained (Perekalin, 2019). Instead of receiving the advertised games software, malware is downloaded to the user's device (ibid, 2019). Dynamic searches for 'cracked games' returned a link to a malicious app disguised as the popular game Call of Duty (McAfee, 2020). The link additionally appeared in YouTube videos. Once downloaded to a device, the app would 'hide' to thwart

detection and deletion, instigate nuisance advertising and act as the installer for other malware (ibid, 2020). Some reputable games manufacturers choose to bypass official app providers and allow their apps to be downloaded from their own website. A user who conducts a web search for a legitimate app is at risk of being directed to a fraudulent site by attackers, and consequently downloading a "malicious copycat app" (Shapland, 2018, quoted in Hern, 2018b, para. 5).

In the context of **RQ2 average usage/impact**, thirty-three percent of the sample use personal devices for online games. As with the issue of copyright protected media content, the survey did not specifically question use of cracked or patched games and results cannot confirm that devices used for gaming brought into the workplace may constitute a risk. Nonetheless, knowledge that gaming takes place on devices may be used to augment risk assessments and instigate dialogue between security managers and employees. A further discussion of data limitations resulting from use of non-specific survey questions is found at 9.3.3.

7.4.5 Gambling, Dating and 'Adult' Applications

Attackers abuse services which attract the most users and popular applications are exploited as attack vectors. Malicious files using the name and design of legitimate dating apps like Tinder can deceive users into downloading malware (Kaspersky, 2020). Other fraudulent dating apps consist of "fake identities managed by chatbots" used to trick users into purchasing premium services (Hu et al., 2019, p. 1). The advertising network on Plenty of Fish dating site was used to infect millions of user's devices with trojan malware (Guruswamy, 2016) and has been found to be vulnerable to data leaks (Moore, 2019).

The ‘adult entertainment’ industry currently occupies position seven, nine and ten on the Global Websites ranking list and a single site can receive three billion visits in six months (Similarweb, 2020). Mobile apps for these highly popular sites are available but cannot be obtained through official channels and must be downloaded from third party sources (Esposito, 2017). In common with other software obtained from unregulated providers, those designed for adult entertainment often contain malicious code. Malware actuated by adult content was responsible for a quarter of all attacks against mobile devices in 2018 (Grustniy, 2018). Threats can be disguised as viewable content or criminals create their own access point for users to view compromised adult material. Gambling and betting are other popular entertainment services and free apps offering casino style games are another source of harm (Proofpoint, 2015). More recently, users have received emails and texts offering credit for online casinos and free games. The messages claim to come from reputable gambling sites but are phishing for credentials or contain malware (iGaming Business, 2020).

7.4.6 Social Media

Social media was referenced in 3.4 as a medium for many harms. Malicious code can be shared via a multitude of methods including infected adverts, images, links and digital media (Hunt, 2019). Third party apps and plug-ins including games and personality tests can be compromised (McGuire, 2019) and any profiles sharing a mutual connection might be affected by a malicious user (Sood and Enbody, 2011). Social media use may threaten corporate IT infrastructure, and employees with many colleagues as friends or followers may exacerbate the risk. Alongside streaming, gaming and messaging, social media apps have been highlighted as those with the most risk to a network (Ashford, 2019) and one in

five organisations has been impacted by malware spread by social media (McGuire, 2019). Results concerning social media are found at 8.5 and social media and the implications from the findings are discussed further at 9.4.

7.4.7 Communication Apps

WhatsApp, Messenger, Snapchat, WeChat, Viber, and Telegram are popular messaging services (Bucher, 2020). Communications apps can deliver semantic messages, video calls and multimedia content, and WhatsApp and Messenger can send and receive PDF, Word, and Excel documents and spreadsheets. Ninety-six percent of respondents use communications apps (see Figure 16, 7.4) and in respect to **RQ2 average usage/impact** malware, scams and other threats can be shared by communications apps. WhatsApp appears to be particularly susceptible to exploitable vulnerabilities (Anstett, 2019; Cuthbertson, 2019b). Other services such as Facebook Messenger (Lutrum, 2019; Palmer, 2017a; Palmer, 2018a) and Telegram Messenger (Palmer, 2018b) have additionally been used to share malware amongst users. Section 8.6 reports the findings for communication apps and the topic is discussed further in 9.3.2.

7.5 The Central Investigation

This section will begin to correlate findings with the research questions by presenting relevant results in association with contemporary literature. The investigation of apps continues with examination of the quantity stored on respondent devices and basic security methods applied by users.

7.5.1 Apps Installed to a Personal Device.

Respondents indicated the number of applications sourced and downloaded by themselves. The question was worded accordingly so that any preinstalled software would not be included, for example, the default web browser, email client or calendar (Mobile App, 2019). Figure 17 (below) illustrates results from seventy-four (N=74) participants.

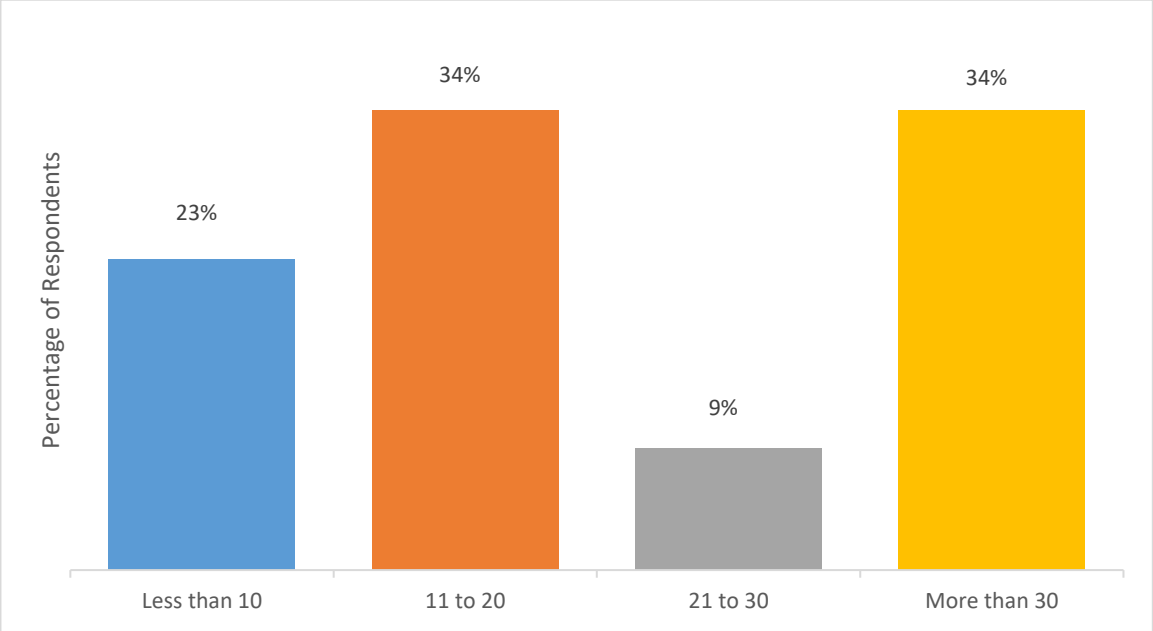

Figure 17. Number of Apps on Devices

The two largest groups of thirty-four percent have between eleven and twenty or more than thirty apps downloaded to their devices. Although the survey asked about the service provided by apps, for example, games, entertainment or communications, no enquiry was made to ascertain the name or specific function of a user's chosen applications.

7.5.2 Outdated Apps

The explanation of apps and associated harms (7.4) discussed potential threats facilitated by use of applications in general and by those performing specific

services. A further app-specific security concern is unused, outdated or unsupported apps present on devices. Statistics show that many users launch an app and abandon it after a single use (Clement, 2019b; Perez, 2016) if it fails user expectation by excessive advertising, poor navigation or technical issues affecting performance (Karnes, 2019). An abandoned app may never be revisited, leaving it dormant and neglected. 'Digital hoarding' might then occur, as users accumulate and store superfluous archaic and unused digital material (Neave et al., 2019, p. 72). Sentimental attachment or laziness and avoidance of spending the time necessary to sort through content prevents users from deleting unused apps or files (ibid., 2019), leaving them stored indefinitely to a device.

An outdated, "dead" app (Guerra, 2015, para. 4), will receive no further support, and can become a security matter if updates are not installed and known vulnerabilities remain unpatched (La Porta, 2018). An additional issue arises if an app is discontinued by the developer and withdrawn from app providers; but continues to be used to provide a service. An application cannot be extracted once installed to a device, and a user may access the original version, despite it receiving no updates or support. If data-copies (a 'back-up') have been made to reinstall lost or damaged data or transfer content, a user may re-install the original version of a withdrawn app each time a device is upgraded (La Porta, 2018). A 'dead' app may continue to be used indefinitely, whilst rendering the device vulnerable to attackers. Figure 18 (below) illustrates the percentage of users who will delete an app or software from devices when it no longer has value and has been 'abandoned'. The sample consists of seventy-one (N=71) respondents.

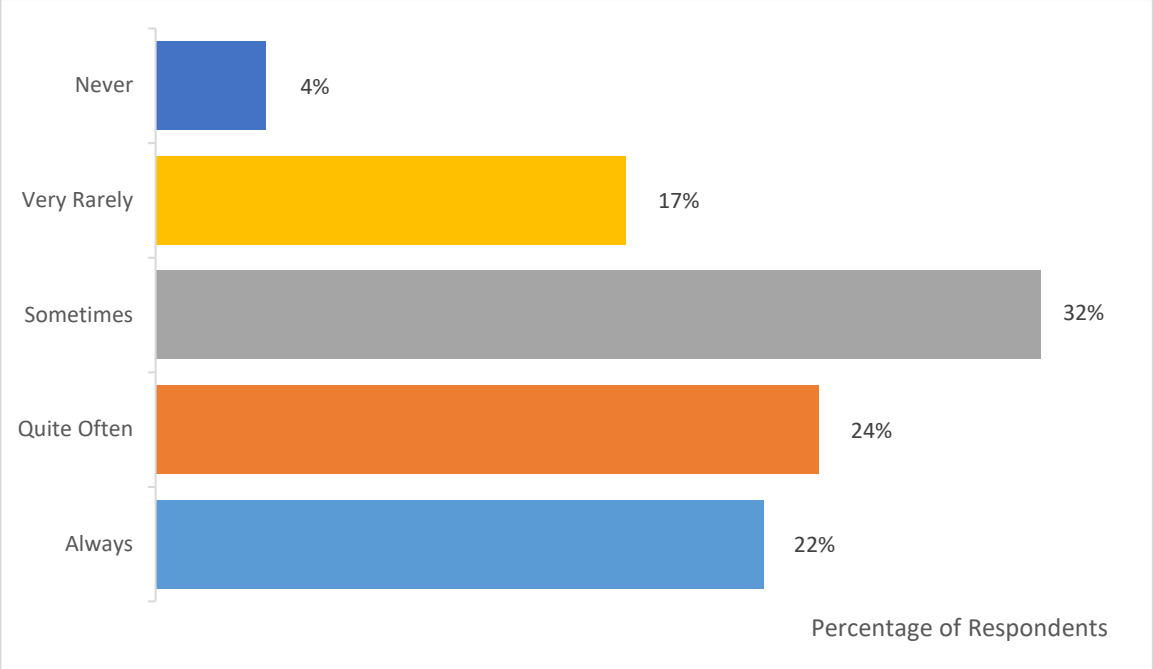

Figure 18. Delete Apps or Software from Devices if not Used

Results show that forty-six percent of respondents 'Always' or 'Quite Often' remove unused items from their devices. Nonetheless, more than half the sample (fifty-three percent) 'Sometimes', 'Very Rarely' or 'Never' delete dormant software concurring with the literature and the concept of digital hoarding. The potential for unsupported apps on devices in the workplace may be a valid concern and is relevant to both **RQ1 actual/perceived risks** and **RQ2 average usage/impact**. An elaboration on outdated software can be found in the discussion chapter at 9.3.6.

7.6 Mobile Device Security

Security for mobile devices may be enhanced by installation of antivirus (AV) solutions and regular maintenance of the operating system and applications by installing recommended updates. In the context of cyber-RAT, these basic user-enabled solutions are capable guardians.

7.6.1 Update When Prompted

Most contemporary devices will automatically *receive* updates, but the user is generally required to respond to a message or prompt to *install* them. Respondents were given a choice of options to indicate their typical reaction whenever a personal device received an update prompt. Figure 19 (below) illustrates the results drawn from seventy-three (N=73) respondents.

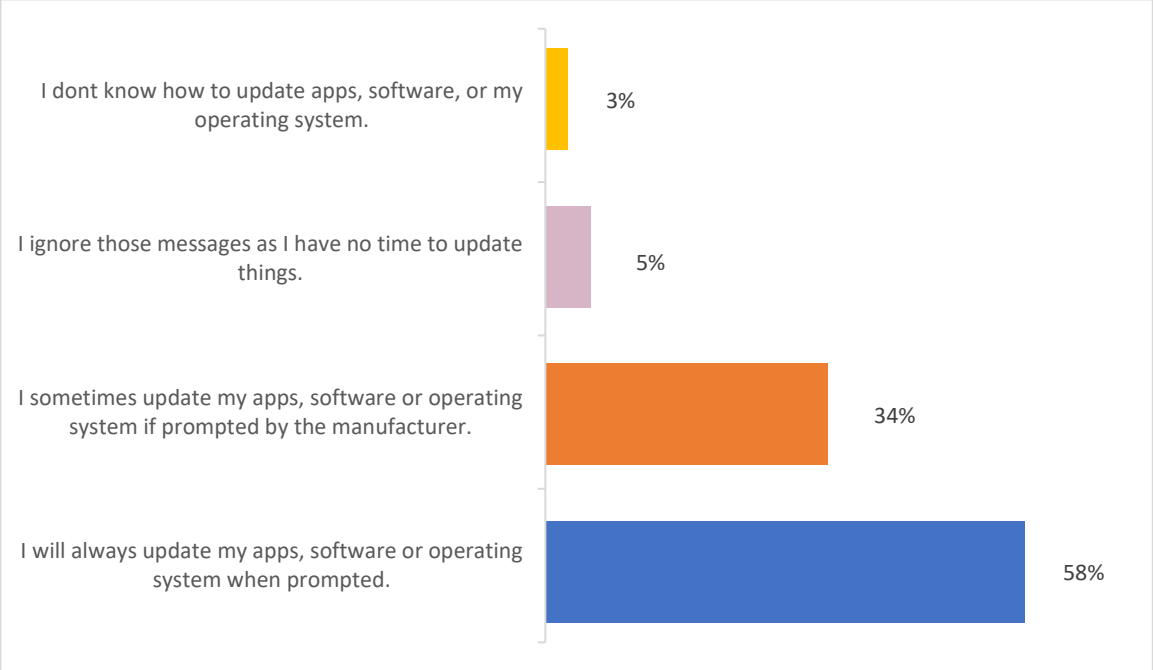

Figure 19. Update Device or Software When Prompted

Figure 19 (above) shows that fifty-eight percent of respondents will always install updates, which indicates an awareness of security amongst users. Despite this, forty-two percent of the sample are not consistent at responding to an installation prompt. The literature (Kaspersky, 2016; Reis, Barth and Pizano, 2009; Zhang, Raghunathan and Jha, 2014) emphasises that software development cannot avoid flaws, and an update will typically repair an identified vulnerability. An operating system or application may not be secure if an update has not been installed, leaving a device at risk of encountering harm. When associated with

results in 7.5.1 illustrating the quantity of apps on respondent devices, findings indicate that irregularly updated software and potentially unsecured devices are present in the financial workplace. These findings are relevant to **RQ2 average usage/impact**. Further discussion regarding updates and associated risk to the corporate network can be found in the discussion chapter, at 9.3.6 and 9.3.7.

7.6.2 Antivirus

Seventy-four (N=74) respondents contributed data to PQ29 which queried use of antivirus AV on personal devices. Figure 20 (below) illustrates results.

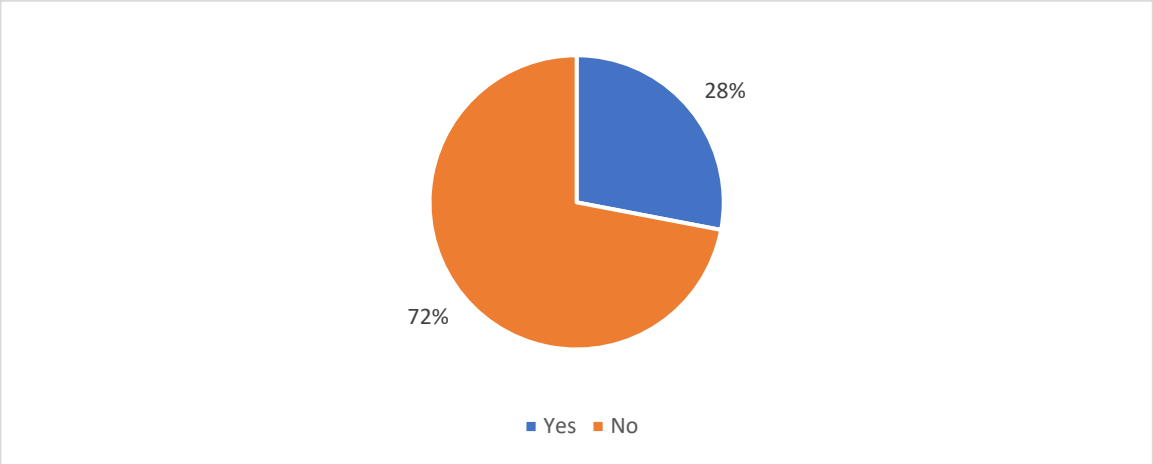

Figure 20. Antivirus Solutions

Seventy-two percent use no additional antivirus solutions to protect personal devices and were invited to explain their choice to forgo AV. Forty-nine users left comments, and a theme became apparent regarding device security. Section 7.6.3 and 7.6.4 evaluate differences observed between users of different operating systems.

7.6.3 iOS Users and Antivirus Solutions

Table 8 (below) illustrates thirty iOS users comments about antivirus solutions.

RN 1	iPhone security.
RN 2	I thought the phone had a level of software built in.
RN 3	I didn't think you can put anti-virus on a phone ....
RN 5	Didn't know I could.
RN 7	Isn't it already installed?
RN 9	Only what comes with the phone.
RN 14	As it's an Apple never felt the need to.
RN 16	Not required on an iPhone.
RN 17	Apple never hacked.
RN 18	It's a waste of time on an iPhone.
RN 19	Never really thought about - though Apple devices are secure?
RN 20	I have not found it useful on Apple devices.
RN 21	I have an Apple iPhone.
RN 26	Didn't think I needed it on my Smart Phone or iPad - I have this on my computer.
RN 27	iPhone.
RN 32	My iPhone, as I understand it is very secure.
RN 34	It's IOS and regard it as safe.
RN 35	I have never had any issues with security and keep my iPhone software up to date.
RN 36	I have an iPhone- it's built in.
RN 42	iPhone.
RN 45	I've an iPhone and don't think it's needed.
RN 48	I don't think it's needed.
RN 49	Just rely on what's on the phone and my network provider.
RN 52	I have all Apple products which only use apps, so you don't need virus protection.
RN 57	You don't need / can't get anti-virus software for an iPhone. All apps are sandboxed and approved by Apple.
RN 58	iPhone - not needed.
RN 66	I don't think I need it for an iPhone.
RN 67	Don't need it.
RN 69	I feel I don't need to. I rely on the software that comes with the phone (iPhone).
RN 71	I don't use it for sensitive material.

Table 8. iOS Users Comments regarding Antivirus

The Apple operating system and the strict controls placed on app developers are renowned for an advanced level of security (Forrest, 2016; Yablokov, 2018) (see 3.7.2). This is reflected in Table 8 (above) where comments suggest that iOS

users are confident that additional security solutions are unnecessary as Apple devices are fundamentally secure. Nine respondents used phrases implying that antivirus was “not needed”. RN18 implied that using antivirus on iOS was a “waste of time”. RN17 claimed “Apple never hacked”, and RN57 stated that “You don’t need/can’t get antivirus software for an iPhone”. Nonetheless, security research emphasises that iOS is vulnerable to malware (Golubev, 2019; Goodin, 2019; Whittacker, 2019) and other harms such as compromised applications, exploitable vulnerabilities in the iMessaging system and malicious email scams (Hay Newman, 2019; Kokh, 2019; Seals, 2020). Forty percent of the overall sample are known to be iPhone users, indicating that iOS has a considerable presence in the financial workplace. In relation to **RQ2 average usage/impact**, the comments indicate over-confidence in the security of personal devices with little user-awareness of the actual harms which may be a threat to them. Thus, user activity on a device with assumed guardianship in place may be a threat to the network.

7.6.4 Users of Other Operating Systems and Antivirus Solutions

The research instrument deliberately made no investigation regarding choice of operating system, therefore all data regarding iOS was divulged spontaneously. It is assumed that other operating systems may include Android, Blackberry, Symbian or Windows although users of other systems made no effort to disclose what device they own. Table 9 (below) illustrates the comments left by users of other operating systems when asked to clarify why they use no AV solutions and implies that antivirus is neglected as it is not a matter of priority. RN6, RN31 and

RN59 do not think about it and RN40 and RN62 do not want to pay for it, which suggests that financial outlay is more important than maintaining security.

RN 6	Don't think about it enough.
RN 10	Didn't know could have them for a phone.
RN 22	Don't mix business and personal.
RN 25	Didn't know it was available.
RN 28	My phone has an automatic one built in.
RN 29	I don't know which one to use.
RN 31	Hadn't really considered it.
RN 37	I couldn't tell you if I do or don't to be honest.
RN 38	I feel my phone is anti-virus free.
RN 40	Not sure which one to use, also don't want to pay for it.
RN 46	Wouldn't know how
RN 53	I don't know what to use and never needed it before.
RN 59	I hadn't thought about it.
RN 61	Everything is backed up and my phone is under warranty and insurance. I can always wipe it and start again, or have it fixed.
RN 62	Don't want to pay.
RN 63	I do not have any sensitive information on my phone - I do not bank using my smartphone.
RN 64	My usage is low risk.
RN 65	Didn't know there was any.
RN 68	Didn't know I could.

Table 9. Users of Other Operating Systems regarding Antivirus

RN22 and RN64 say their internet activity is low risk, intimating caution when accessing content. Nonetheless, respondent data confirmed that both RN22 and RN64 engage in social media and have more than one communication app installed to devices. Thus, assertion of low risk may imply unfamiliarity with actual risk enabled by the internet. RN61 stated that because his data has been copied and stored elsewhere, antivirus is not necessary since the phone can be “wiped”

and “fixed”. For RN61, the preference is for corrective action instead of proactive prevention. Since an additional outcome of a compromised phone may be the impact on other systems, networks or devices, RN61 may be indifferent to the effects of personal activity or unaware of the overall potential for harm. Thus, in relation to **RQ1 actual/perceived risks,** a lack of consideration towards guardianship may be an actual risk. In the context of **RQ2 average usage/impact**, the failure to consider guardianship whilst continuing with routine activity where convergence may take place is a potential risk to the corporation.

7.6.5 iOS and Other Operating Systems in Relation to RQ1 and RQ2

Table 8 (7.6.3) and Table 9 (7.6.4) illustrate differing attitudes towards device security, and both are relevant to the central investigation. iOS users have some (apparent) knowledge of the expected security of an Apple system and apply this to justify no additional protection. Therefore, in respect to **RQ1 actual/perceived risks**, a blasé attitude to device security may constitute an actual risk. In contrast, those using other operating systems appeared uninformed or uninterested about antivirus for mobile devices, admitting to ignorance of availability and concern about financial outlay instead of the added value of a secure device. In accordance with **RQ1 actual/perceived risks**, an obtuse attitude to device security may additionally constitute an actual risk. In respect of **RQ2 average usage/impact**, seventy-two percent of the sample conduct personal internet activity on devices with no protection against threats introduced via online mechanisms. Regardless of the actual effectiveness of antivirus against unknown or sophisticated malware, users who do not apply basic guardianship may be a risk to corporate networks. Further elaboration on the challenge and possible

solution for enhancing cyber awareness for users who consider they are adequately protected, is discussed in Chapter Nine at 9.7.3.

7.7 Conclusion to Recording the Data and Content Analysis

This chapter has focused predominantly on introducing the sample of financial employees and examining their personal technologies alongside the routine digital activities they are used for. Results have been recorded using descriptive statistics so that trends in data might be recognised and explored further in the following chapters. Findings thus far indicate that activity using applications may be relevant to **RQ2 average usage/impact,** and the explanation of associated harms (7.4) was necessary so that the cyber-RAT framework may be applied going forward. Analysis conducted within the parameters of the research questions has ascertained that outdated or discontinued apps stored to devices may be actual risk (**RQ1 actual/perceived risks**) supported by evidence that respondents install many apps to devices and do not always remove them once they are no longer in use. Basic guardianship in the form of antivirus and regular updates have been examined and a distinct trend identified in attitudes towards security. This trend of assumed guardianship in users of iOS systems will be explored further throughout the ensuing analysis. The next chapter (Chapter Eight) will continue to record and extract value from the results whilst guiding the narrative towards the resolution of the research questions.

Chapter Eight: Analysis and Interpretation

8.1 Introduction

The analysis throughout Chapter Eight is driven by the central investigation. The narrative documents observed behaviours, providing qualitative interpretation to associate user activity with the literature. The chapter begins by dividing the sample into categories according to interaction with the internet and technology. Whenever results indicate a behavioural trend, new data samples with similar tendencies are grouped and interpreted in association with contemporary security research and academic works. Findings are illustrated as either a percentage of each specific dataset or a measure of individual users. Some samples are very small, dependent on the quantity of respondents who provided data, but are included due to the relevance to **RQ1 actual/perceived risks** and **RQ2 average usage/impact**. To illustrate with perspective, the overall sample of seventy-six (N=76) is not large but represents an estimated twenty-seven organisations. Therefore, even the smallest sample discussed in Chapter Eight may indicate users from more than one company. Since academic study examining insider threat states how an organisation can only be as strong as the weakest link (Colwill, 2009), a single employee inviting risk may compromise an entire enterprise. Any indication of this in the findings adds value to the results.

Chapter Eight is arranged as follows: Section 8.2 examines digital activities drawn from themes observed in the literature and evaluates the sample in the context of actual risk created by employees. Section 8.3 considers use of personal devices connected to the corporate network and assesses digital activity in the workplace

and personal space. Section 8.4 expands the investigation of the dataset connected to the corporate network to include device security and applications. In 8.5, the narrative returns to the complete sample to assess employee use of social networks, and harm via social media. Section 8.6 records findings relating to communications apps including WhatsApp, Facebook Messenger and Snapchat. Section 8.7 and 8.8 are devoted to **RQ3 IoT unexplored risk**. At the end of each section the findings are summarised to specify the relevance to the research questions.

8.2. Digital Activity in the Workplace

Participant Question PQ29 invited respondents to indicate how often they would undertake specific digital activities in the workplace. Choices were 'Always', 'Quite Often', 'Sometimes', 'Very Rarely' or 'Never'. The intention of PQ29 was to ascertain whether potentially harmful actions occurred on company premises in the vicinity of other users devices and systems connected to the corporate network. So that trends in behaviour might be identified and applied to **RQ1 actual/perceived risks** and **RQ2 average usage/impact**, the subsequent questions asked whether personal or work devices were used for workplace activity and those who indicated use of company devices were invited to specify type of device. Seventy-four (N=74) respondents provided data and three groups were formed from the results:

- Group A: Activity using only company issued devices.
- Group B: Activity using both personal and company issued devices.
- Group C: Activity using only personal devices.

Throughout 8.2, charts will visually illustrate data to accompany the interpretive narrative beginning with Figure 21 (below) which illustrates the percentage of respondents in each group. Findings begin with examination of Groups A and B and use of company issued devices for digital activity in the workplace.

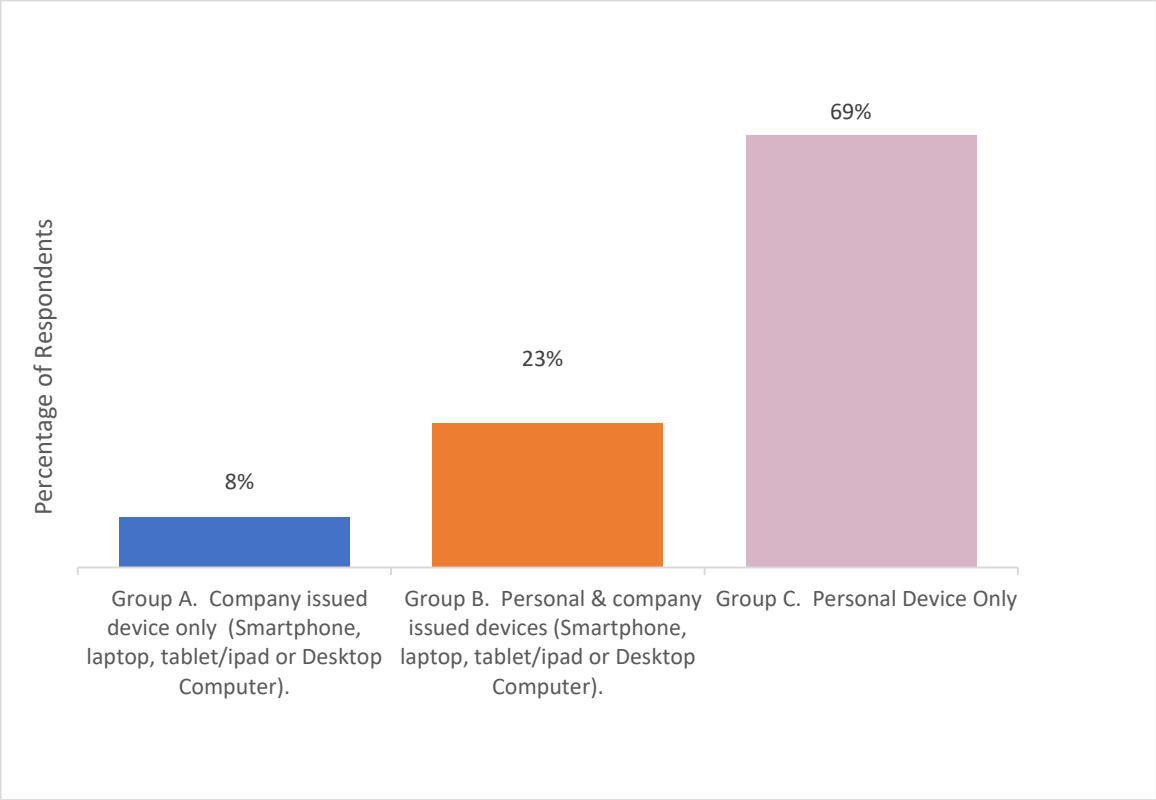

Figure 21. Devices used by Groups A, B and C

Eight percent of respondents use only a company issued device and twenty-three percent use both company and personal devices. Although small datasets, the combination of Groups A and B suggest that thirty-one percent of the overall sample acknowledge use of company devices to conduct potentially harmful digital activity in the workplace. This is relevant to **RQ1 actual/perceived risks**, since devices provided by an organisation for work purposes may be connected to the corporate network and/or have access to corporate data.

8.2.1 Types of Company Issued Devices

Figure 22 (below) illustrates the percentage of respondents using specific company issued devices. Sample size is thirty-one (N=31).

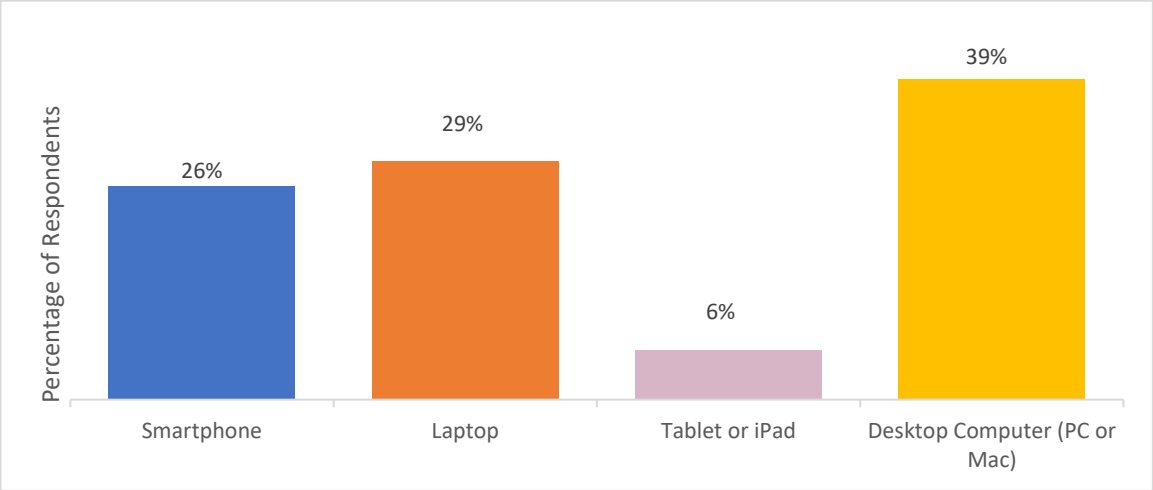

Figure 22. Company Issued Devices used for Digital Activity

Figure 22 (above) shows that the desktop computer and laptop are the most common devices provided by organisations, possibly due to the larger screen facilitating preparation and viewing of documents and spreadsheets. Twenty-six percent use a company smartphone, most likely intended for business calls and enable remote working using cloud facilities when out of the office.

8.2.2 Workplace Activity

All digital activities examined in PQ29 required internet access, thus it is plausible that devices were connected to the corporate network whilst digital activity took place. Figure 23 (below) illustrates digital activity of Group A who used only company devices, followed by Figure 24 illustrating Group B, users of personal and company issued devices. Group A consists of six respondents (N=6) and Group B contains seventeen respondents (N=17).

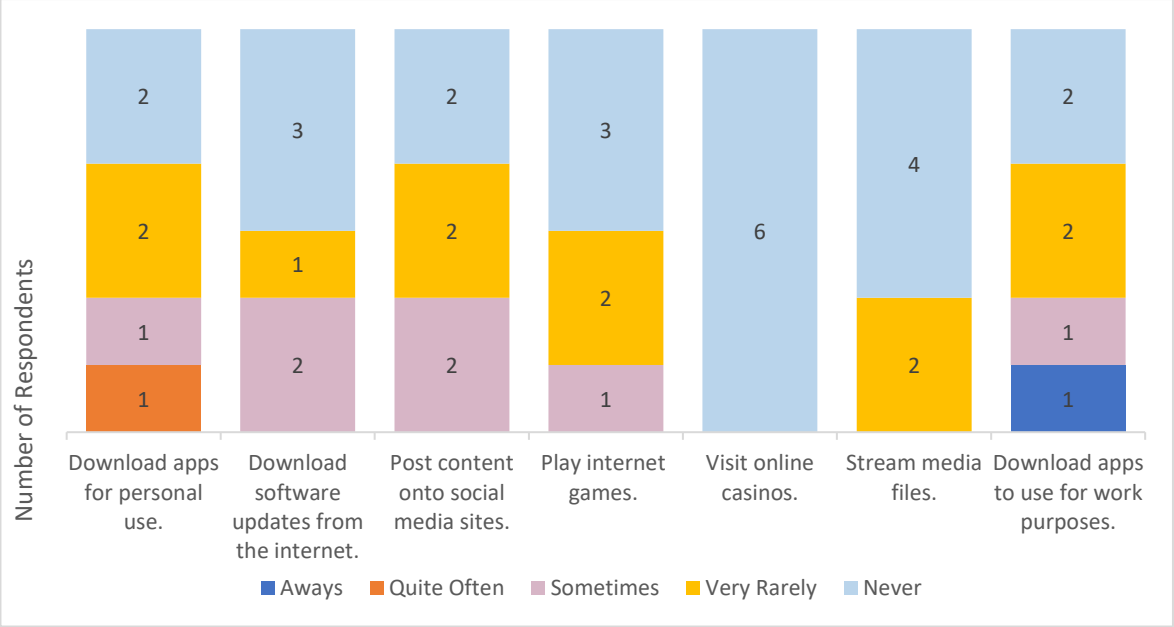

Figure 23. Group A: Workplace Activity using Company Devices

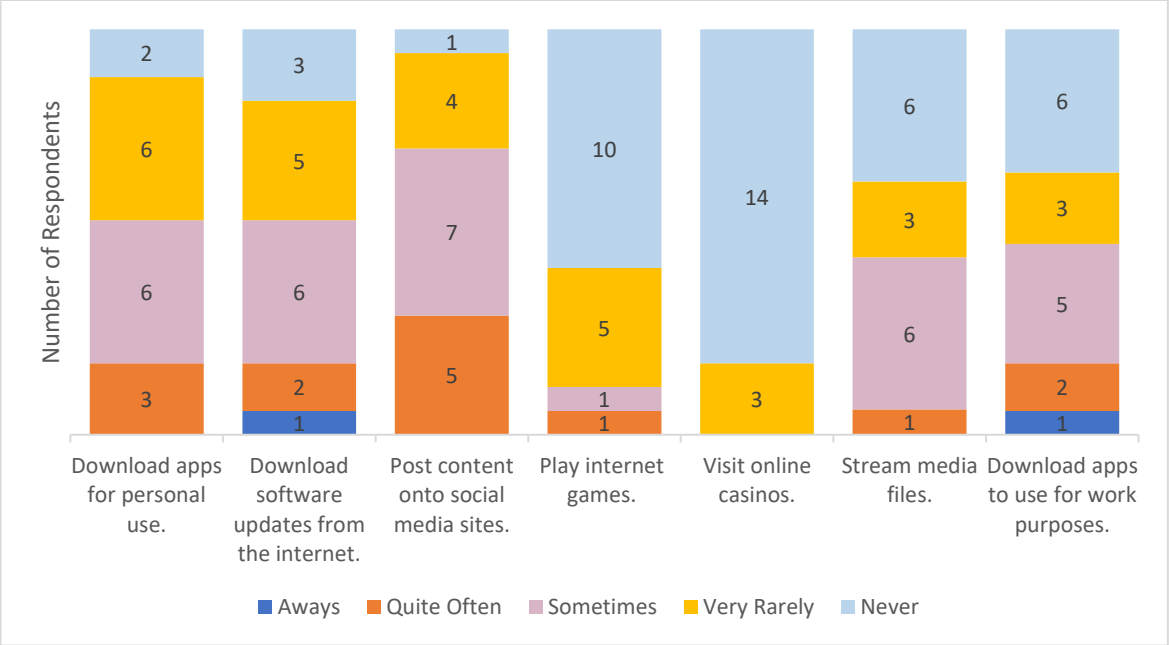

Figure 24. Group B: Company Issued and Personal Devices

Figures 23 and 24 (above) illustrate that the number of respondents in both groups who 'Never' conduct potentially harmful activity is significantly higher than those who stated otherwise. Nonetheless, in regard to **RQ1 actual/perceived risks**, the value of the data is not what *does not* take place, but evidence of what

does occur, regardless of regularity. The research instrument was limited by not providing a definitive measure of frequency and each respondent was forced to be subjective towards the frequency markers of 'Always', 'Quite Often', 'Sometimes' and 'Very Rarely'. To illustrate, one social media user may consider that posting content once a month is an occurrence taking place 'Very Rarely'. Another user might quantify the same time frame as 'Quite Often' since it takes place on a regular monthly basis. 'Very Rarely' might additionally indicate a regular activity occurring less frequently than other internet activities. For example, online gaming might take place daily, but using an online casino only happens at the end of the month when a salary is paid. Despite taking place on a regular monthly basis, the user quantifies the gambling as 'Very Rarely'. The digital activities surveyed in PQ29 have capacity to introduce harm (see 3.3.2 and 7.4) and affirmation of 'Very Rarely' still indicates that a potentially risky activity takes place on occasion. Respondents who stated 'Always', 'Quite Often', 'Sometimes', or 'Very Rarely' are therefore relevant for further examination. The limited results in Group A reflect the small number in the sample. If the number of respondents had equalled that of Group B, those answering 'Always', 'Quite Often' and 'Sometimes' may have shown a higher rate of occurrence.

8.2.3 Software Updates and Downloading Apps

Seventy-four percent affirmed 'Always', 'Quite Often', 'Sometimes', or 'Very Rarely' to downloading software updates from the internet. This question was specifically targeted towards users of laptops and static desktop computers and Figure 22 (8.2.1) confirmed that these devices have a significant presence in the corporate workspace. Results evidence that employees are downloading updates to corporate systems and in respect to **RQ1 actual /perceived risk,** this may be

an issue of concern to security managers. Not only in respect of shadow IT (see 3.9.7) and a technological infrastructure created without knowledge or authorisation from IT managers (Carter, 2015; Chapman, 2015; Froehlich, 2015) but the potential for downloading malware to company systems. Popular productivity software, commonplace in many office environments is a soft target favoured by attackers who dupe users into installing legitimate updates infected with malware (Invision, 2019; Sentinel One, 2016; Symantec, 2018) (see 3.3.2). Employees with technical proficiency may consider basic system maintenance as a simple activity to assist with security or productivity. Nonetheless, software installation or system support maybe outside the remit of most employees or require authorisation from a designated manager.

Malware disguised as an application is a valid threat and tools, lifestyle and entertainment are categories frequently targeted by criminals due to user popularity (Symantec, 2019) (see 3.7.3 and 7.4). Sixty-five percent of respondents affirmed that applications for work purposes are ‘Always’, ‘Quite Often’, ‘Sometimes’, or ‘Very Rarely’ downloaded to company devices. This may confirm the literature as apps intended to assist with office work might be categorised as ‘tools’. Eighty-three percent additionally claimed that apps for personal use are ‘Quite Often’, ‘Sometimes’, or ‘Very Rarely’ downloaded to company devices. Users accustomed to regularly downloading mobile and desk-top applications may instinctively acquire additional software to assist with efficiency or to provide a distraction during breaktime and are relevant to **RQ1 actual/perceived risk**. The data is limited as respondents were not required to categorise apps downloaded in the workplace, but those for personal use might

include games, or viewing or listening to media and may be considered as ‘entertainment’ apps. As company devices are assumed to be connected to the corporate network, employees downloading apps for work and personal use are not only indicative of shadow IT (3.9.6) but may place the organisation as suitable target at risk of convergence by an instrument to extend the reach of an attacker.

8.2.4 Use of Apps

Findings for Groups A and B show that alongside *downloading* apps, digital activity requiring *use* of apps is taking place using company devices. Apps and associated harms were discussed at length in 7.4, and Figures 23 and 24 (8.2.2) illustrate that categories seemingly capable of placing users as suitable target and introducing risk of convergence are accessed with varying regularity. These include social media, games, streaming and casinos, all known to be vectors for distributing malware (see 7.4). In the context of **RQ1 actual/perceived risks**, potentially unsafe activity using a work device is an actual risk posed by employees due to a connection to the corporate network or access to critical data.

8.2.5 Groups A and B: Occupations

Employee workplace digital activity presented in Figures 23 and 24 (8.2.2) is significant to the central investigation and findings from Groups A and B have direct relevance to **RQ1 actual/perceived risks** and possible threat to an organisation. Demographic data was examined to ascertain occupations of Groups A and B to identify which levels of the corporate hierarchy undertake digital activities using company devices. Figure 25 (below) illustrates occupations and percentage in each role. The sample size is twenty-three N=23).

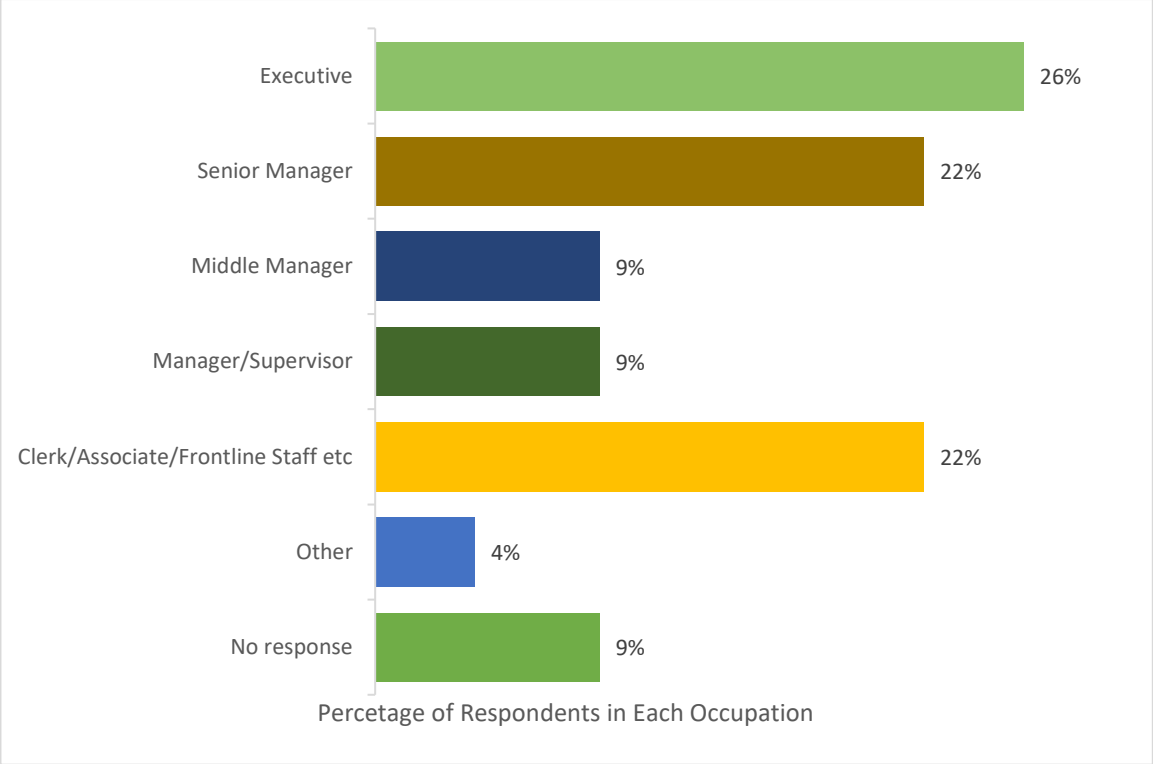

Figure 25. Occupations of Groups A and B

8.2.6 High-Level Personnel and Workplace Digital Activity

Findings illustrated in Figure 25 (above) suggest that forty-eight percent of respondents in Groups A and B using company devices are executive personnel and senior managers. This is of interest as high-level staff will have access to core systems and customer data and might be assumed to have enhanced awareness of cyber threat to the financial sector. Executive and senior level staff were subsequently examined as a new sample to ascertain type of activity undertaken by those with responsibility for corporate data. Figure 26 (below) illustrates the results. Only activities taking place 'Always', 'Quite Often' , 'Sometimes' and 'Very Rarely' are represented and where the chart shows a limited number of participants for a particular activity, all other respondents recorded 'Never' in the survey answer field.

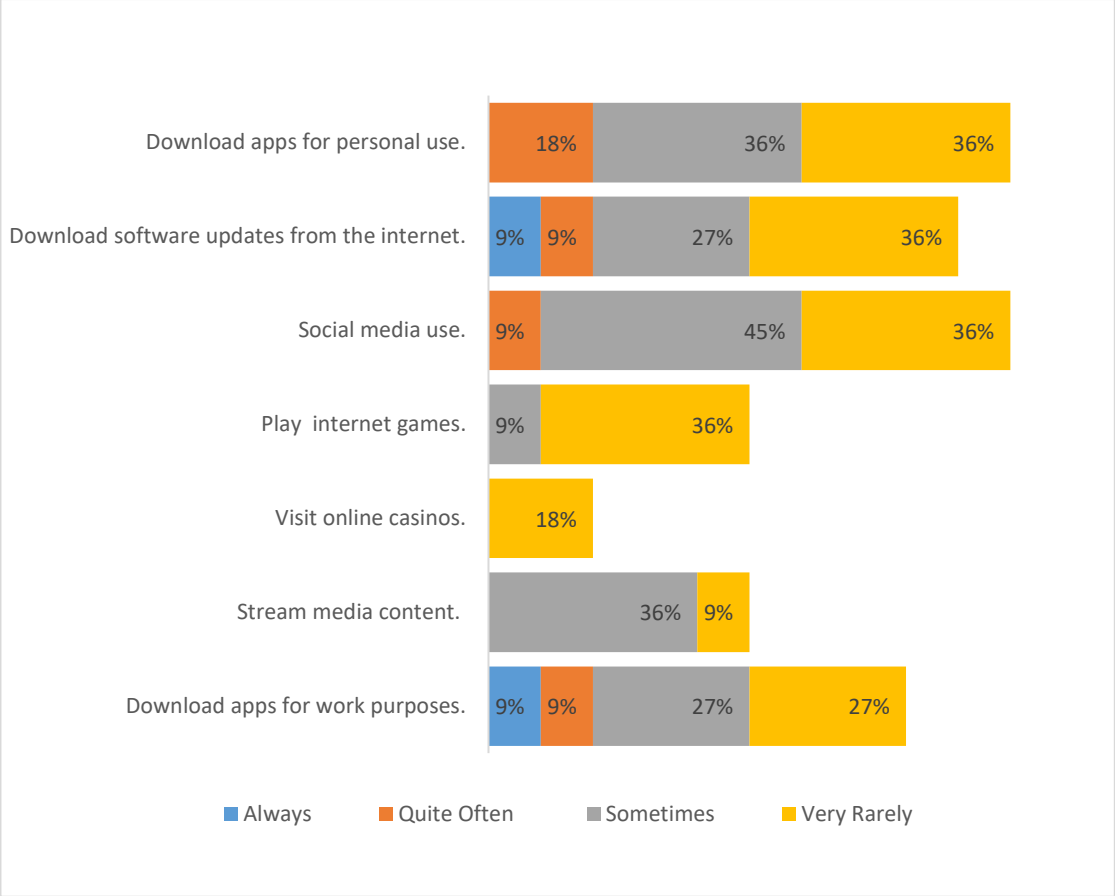

Figure 26. Senior Staff from Groups A and B using Company Devices

Figure 26 (above) demonstrates that all categories occur with varying regularity ranging from 'Always' to 'Very Rarely. Common activities include use of entertainment apps and social media and more regular downloading of applications for work and personal use is evident. High-ranking staff may consider their seniority affords 'flexibility' with company policies involving internet use, but results imply digital activity is not being equated with risk of cyber-attack. This may be lack of awareness regarding the range of cyber threats or a failure to comprehend that devices connected to the network may give direct access to critical data. In respect to **RQ1 actual /perceived risk**, senior-level behaviour may be an actual risk to a corporation and the discussion in 9.7.2 elaborates on high-ranking personnel as an insider threat.

8.2.7 Summary of Groups A and B in Relation to RQ1

Potentially unsafe routine digital activity takes place in company space, conducted by personnel throughout the corporate hierarchy including those in executive and senior positions. Devices intended for business activity may be connected to enterprise IT infrastructure or have direct access to company files and critical data. Use of corporate tools to receive internet downloads and access entertainment applications may position organisations in the role of suitable target. Convergence with offender or instrument to extend the offender's reach is possible. In the context of **RQ1 actual/perceived risks**, digital behaviour of the small sample consisting of Groups A and B may constitute an actual risk to a financial corporation.

8.3 Group C: Users of Personal Devices

The aim of **RQ2 average usage/impact** was to examine how employees use personal devices and theorise areas of risk which may not be addressed by traditional risk management practices. Group C consisted of fifty-one users who conduct all workplace activity using personal devices. Of this group, sixty-seven percent confirmed that personal devices 'Always' and 'Sometimes' connect to the corporate network. Sections 8.3 and 8.4 will examine device use which might place an organisation in position of suitable target as a result of routine activity. Regularity of connection is not pertinent since a device granted *any* access to the corporate IT infrastructure has relevance to the central investigation.

In addition to sharing harm *whilst* connected to a corporate network, malware may spread if a device is compromised by exposure during online activity elsewhere

and later granted access to corporate systems. Online activities conducted in the personal space of respondents in Group C are therefore relevant to the investigation and 8.3.1 will first consider 'personal space online behaviour' before continuing with the examination of workplace digital activity.

8.3.1 Routine Internet Activity in the User's Personal Space

'Personal space' is any place or time where the user is at liberty to indulge in unrestricted online activity. Examples are the user's living accommodation or a daily commute using public transport. Online activity is unregulated in personal space and moderated only by individual guardianship. Connecting a device to a corporate network after potentially unsafe personal activity is relevant to **RQ2 average usage/impact** and it is necessary to ascertain whether activities include those recognised as potential distributors of malware or other harms.

Figure 11 (7.3.2) illustrated findings from Participant Question 4 where routine personal device usage included eight activities where users may be placed in position of suitable target at risk of convergence. These are downloading apps, social media, gaming, streaming content, online casinos, 'adult content', use of communications applications and dating apps. Figure 27 (below) illustrates the percentage of respondents from Group C who undertake each activity. The sample size is thirty-four (N=34).

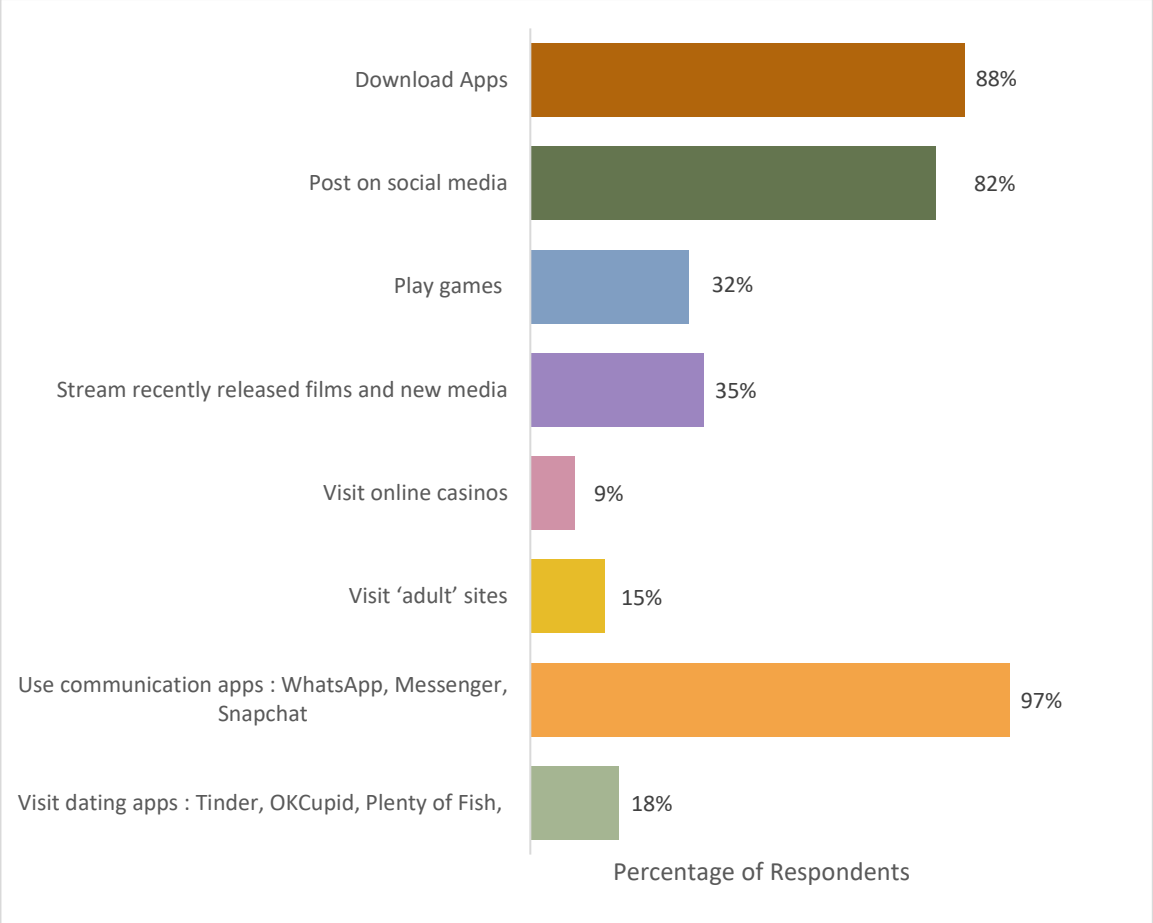

Figure 27. Group C: Routine Digital Activity in Personal Space

Figure 27 (above) illustrates that all potentially unsafe app-based activity discussed in in 7.4 is undertaken by employees in personal space, using devices which accompany the user to the workplace. Respondents in Group C confirmed that devices are connected to corporate networks, thus, the potential for any unknowingly accessed harm to compromise the IT infrastructure and corporate assets is a theorised risk in accordance with **RQ2 average usage/impact**. Harm may also be shared to other devices via SMS, Bluetooth and communication apps and is an additional unmitigated risk relevant to **RQ2 average usage/impact**. In respect of *actual* risk, employees' devices utilised for unrestricted 'unsafe' personal activity brought into the financial workplace may be a threat to the

corporate network and these results additionally contribute to **RQ1 actual/perceived risks**.

8.3.2 Group C: Digital Activity Whilst Connected to the Corporate Network

This section (8.3.2) will examine Group C and digital activity occurring in the workplace using devices connected to the corporate IT infrastructure. Two respondents from Group C claimed to undertake no digital activity at work, and one participant passed the question. Figure 28 (below) demonstrates the percentage of respondents from a sample of thirty-one (N=31).

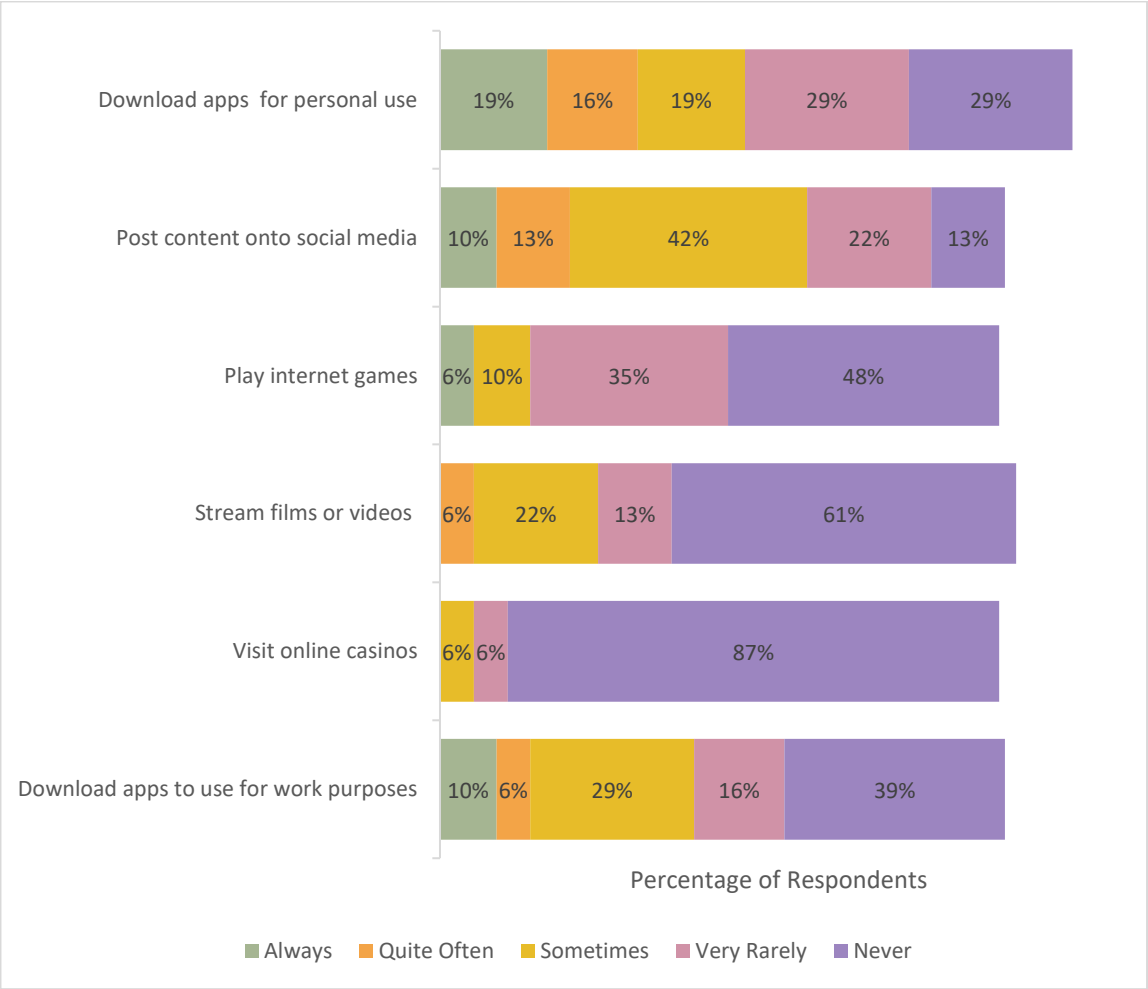

Figure 28. Group C: Digital Activity whilst Connected to the Network

Figure 28 (above) reveals that potentially unsafe activities take place with varying regularity. The most common is social media, with only four respondents claiming that no access to social networks takes place. Streaming content, gaming and downloading apps for personal and work use are additionally well represented in the results. Participants were not surveyed about use of dating or adult apps as it was assumed that these activities would not occur in the work environment and that respondents would be unlikely to admit to using such apps whilst at work.

When results in Figure 28 (above) are compared with Figure 27 (8.3.1) it is apparent that the number of respondents engaging in each activity in the personal/private space is analogous to the quantity conducting the same activity in the workplace. It is plausible that respondents continue using the same applications at work as they were using at home or during their commute. Theoretical examples are an employee watching a film during the morning commute who continues viewing during quiet times at work. An online game played whilst travelling on public transport might be accessed throughout during the working day. In some instances, the quantity of users carrying out the activities in the workplace exceed those who partake in personal space. For example, eleven respondents play games in personal space, and sixteen 'Always', 'Quite Often', 'Sometimes', or 'Very Rarely' play at work. This may suggest that a user does not play at home but at work might compete with colleagues or play alone to pass time during quiet periods. Thirty respondents stated that they download apps as routine activity, and this is reflected in workplace activity where twenty-two users download apps for personal use and nineteen download apps for work purposes.

Other than the activities of streaming and online casinos where more respondents answered 'Never' when asked if these take place at work, findings suggest that more employees conduct potentially harmful activity in the workplace than those who do not. This is particularly evident in results for social media and downloading apps for personal use. As respondents have their personal devices with them in the workplace, they may feel at liberty to continue with routine digital activities when opportunity arises. As an additional theorised risk relevant to **RQ2 average usage/impact**, by conducting the same activities at work as in personal space a user remains consistent as suitable target. By connecting the device to the network, fluidity of cyber-RAT extends suitable target to the organisation which is also at risk of convergence with offender or instrument extending reach.

8.3.3 Group C: Occupations

To ascertain which levels of the corporate hierarchy conduct workplace digital activity, demographical data for Group C was examined. Respondent occupations are illustrated in Figure 29 (below). Four users did not state an occupation and the sample is thirty (N=30).

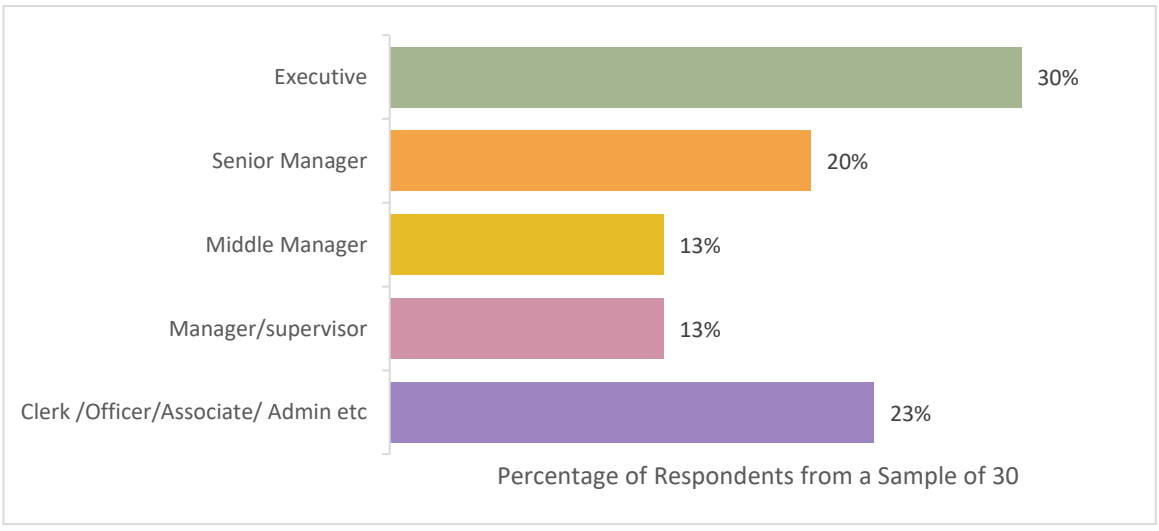

Figure 29. Group C: Occupations

In accordance with results for Groups A and B (see 8.2.6) the largest group conducting workplace digital activity is executive personnel. As key personnel receiving letters of invitation were predominantly executives, it might be assumed that the overall sample would contain a significant number of senior staff and subsequently executives would be the largest groups in the results. However, Figure 8 in 7.2.6 illustrates that executives are the smallest demographic in the overall sample. Thus, the findings in 8.3.2 suggest that executive personnel may not be aware of the potential risk of unsafe personal activity impacting on corporate networks. Alternatively, they may believe themselves to be adequately protected, either by corporate security systems or enabled device guardianship.

8.3.4 Summary of Group C in Relation to RQ1 and RQ2

Group C is not a substantial dataset, but results show that all respondents display some potentially unsafe behaviours whilst connected to the network. These occur with sufficient regularity to suggest that if guardianship is not enabled then victimisation might occur. Small organisations often employ less than fifty employees (OECD, 2020) hence, a workforce of similar size to Group C may plausibly contain a comparable number of personnel engaging in similar conduct. Any organisation is only as strong as its weakest link (Colwill, 2009; Verizon, 2019) and a single employee may unwittingly instigate an attack. The literature maintains that an attacker need only succeed once when attempting to penetrate a network (Symantec, 2016, p.6). Therefore, an activity taking place ‘Very Rarely’ may still have capacity to compromise organisational systems.

Group C represented forty-five percent of the overall sample, demonstrating that almost half the participants connect devices to the network *after* they have been used for potentially unsafe internet activity in the users' personal space. In respect to **RQ2 average usage/impact**, users placed in position of suitable target by routine personal activity may extend risk of victimisation to the IT infrastructure and subsequently the organisation. Findings suggest that the extent of workplace digital activity is similar to that observed in personal space. Hence, users who access specific applications in personal space may be re-visiting applications whilst at work, thus bringing risk of convergence into the workplace.

In respect of **RQ1 actual/perceived risks**, social networks are acknowledged as a common attack vector (see 3.3.3) and a high volume of employees accessing social media in the workplace may be of concern. Gaming and streaming can cause harm, dependent on how the user chooses to access their content (see 7.4.2 and 7.4.4) and applications can be used as a medium to introduce malware (see 7.4). Employees using the corporate network as the method of connectivity to conduct these activities may constitute an actual risk to the organisation. Staff across all levels of corporate hierarchy are seen to conduct unsafe behaviour but senior personnel comprising of executives, directors, and business owners represent the largest numbers of respondents in the Group C dataset. The most senior personnel typically have responsibility for an organisation and corporate assets in the form of critical data, thus, executives may generally be assumed to demonstrate advanced cyber awareness. Findings suggest that any policies governing personal workplace activity may be overlooked by executive staff and imply a general lack of awareness regarding suitable target and internet offender

or instrument-in-technique. Hence, in respect of **RQ1 actual/perceived risks**, senior staff may pose an actual risk to the organisation. A designated IT department may be responsible for maintaining cyber security, but system managers are undermined if higher-ranking staff do not comply with safety measures because they do not have the same awareness of risk (Werlinger, Hawkey and Beznosov, 2009). Subsequently, instead of enabling guardianship, executives may be placing the organisation at risk of convergence.

8.4 A Further Exploration of Devices Connected to the Network

Findings thus far have established that devices connected to the network may have applications installed which are used for potentially 'unsafe' activity and have capacity to introduce harm. This section will further evaluate Group C, beginning with the number of applications users have downloaded to their devices, before examining basic guardianship in the form of antivirus and system updates.

8.4.1 Number of Apps on Devices Connected to the Network

Applications installed to devices connected to the network are relevant to both **RQ1 actual/perceived risks** and **RQ2 average usage/impact**. Table 10 (below) illustrates the number of apps for thirty-three (N=33) members of Group C.

Group C.				
Number of Apps on devices connected to the network	**Less than 10**	**11 to 20**	**21 to 30**	**More than 30**
Percentage of Respondents	24%	27%	9%	39%

Table 10. Number of Apps on Devices Connected to the Network

Table 10 (above) illustrates that thirty-nine percent of Group C have more than thirty self-selected applications on their devices. The data is limited as the research instrument did not request an exact number, but the literature suggests that average smartphone users may have approximately eighty applications installed (Sydow and Cheney, 2018). Devices with many apps may be exposed to malware masquerading as legitimate software (3.7.3) or have outdated or dead applications (7.5.2) particularly if the user is prone to "digital hoarding" (Sweeten, Sillence and Neave, 2018, p. 54). A device in the workplace carrying numerous apps may be an actual risk as suggested by **RQ1 actual/perceived risks**.

8.4.2 Group C: Device Security – Updates

Section 8.3.2 documented workplace digital activity of Group C and results showed that all categories of potentially unsafe activities take place whist devices are connected to the network. It was therefore necessary to ascertain whether users are employing basic device security measures to enable guardianship. Table 11 (below) illustrates responses given by Group C when asked if updates were installed to applications or operating systems when prompted. One respondent passed the question, and the sample size is thirty-three (N=33).

Group C.			
Update Apps and Operating Systems	**Always**	**Sometimes**	**Never**
Percentage of Respondents	61%	27%	12%

Table 11. Update of Apps and Operating Systems

Thirty-nine percent of Group C 'Sometimes' or 'Never' respond when an update prompt is issued, suggesting that devices connected to the internet may not have

basic guardianship enabled. Some devices have facility to automatically install an update, but users may choose to avoid them for a variety of reasons. An update can impair device functionality whilst in progress and disrupt a user's lifestyle (Reinhard, 2016). Automated updates may also waste data if downloaded without using Wi-Fi and drain battery power if occurring often (Gadgets 360, 2017). Downloads may also monopolise bandwidth on a limited Wi-Fi connection (Crookes, 2016) and users who find automated installation inconvenient may disable the feature on their devices. A software update can often modify or remove features and concern that a favourite app will be irrevocably altered may incite a user to delay an update until any performance issues are reported by others (Lewis, 2019). If a user dislikes proposed new features and instead prefers the current version, they may continually avoid the update despite any safety recommendations by the manufacturer (Ryan, 2015). The data shown in Table 11 (above) suggests that some users connected to the network may be choosing to refuse a security update as a preference for performance instead of safety.

8.4.3 Device Security and Digital Activity

An update is generally intended to manage any identified security issues and will often improve the functionality of a piece of software. A device not regularly installing updates may be vulnerable to internet threats and other harms. Thus, respondents from Group C who stated 'Sometimes' and 'Never' were examined to theorise possible risk to devices not receiving regular updates. Table 12 (below) shows number of apps installed and the presence of any antivirus solutions. A cross indicates the type of digital activity undertaken by each respondent in personal space before connecting the device to the corporate network.

RN	Number of Apps	Updates	Anti-Virus	Social Media	Games	Streams	Casinos	Adult Content	WhatsApp etc	Dating
RN 6	11 to 20	Sometimes	No	x	x	x	x	x	x	x
RN 10	11 to 20	Never	No	x					x	
RN 12	< 10	Sometimes	Yes						x	
RN 17	> 30	Sometimes	No	x	x	x			x	
RN 20	11 to 20	Sometimes	No	x					x	
RN 21	11 to 20	Sometimes	No	x		x			x	
RN 31	> 30	Sometimes	No	x					x	x
RN 40	> 30	Sometimes	No	x		x			x	x
RN 48	11 to 20	Never	No	x		x			x	
RN 49	< 10	Never	No						x	
RN 54	< 10	Never	Yes			x			x	
RN 59	11 to 20	Sometimes	No	x	x				x	
RN 61	11 to 20	Sometimes	No	x		x	x	x	x	x

Table 12. Group C . Irregular updates and digital activity

Table 12 (above) shows that all categories of unsafe behaviours take place despite many users, individually denoted as research number (RN), applying irregular updates and using no antivirus. Social media, communication apps and streaming are most prevalent but online casinos, adult content and dating sites are also accessed. In the context of cyber-RAT and suitable target, RN6 and RN61 are examples of employees who may be at risk of convergence since routine activity includes the majority of potentially unsafe activities and capable guardianship may be inadequate. RN61 is an iPhone user and may thus consider that sufficient guardianship is present (see 7.6.3). Nevertheless, iOS may be vulnerable to sophisticated threat (Golubev, 2019; Goodin, 2019; Hay Newman, 2019; Kokh, 2019; Seals, 2019) and guardianship may have limited capability when the device is used for 'unsafe' digital activities. In respect to **RQ1 actual/perceived risk** and **RQ2 average usage/impact,** a user partaking of

unrestricted ‘unsafe’ behaviour believing that adequate guardianship is present may constitute an actual risk when the device is brought into the workplace.

RN6 also routinely undertakes ‘unsafe’ behaviours in personal space regardless of adequate guardianship but is not an iPhone user with the (apparent) inbuilt security. Thus, RN6 may not be aware that an update includes essential safety features and is important to maintain system security. Alternatively, this respondent may deliberately avoid any proposed modification of a favourite app or system. Proceeding with potentially unsafe behaviours without adequate guardianship may suggest that the user has not experienced loss and does not associate personal use with risk of harm as proposed by Rughiniş and Rughiniş (2014). It is possible that RN6 subscribes to paid services for all entertainment, media access, adult content and other online amenities and may subsequently consider that paid services provide adequate protective measures. Nonetheless, irregular updates will prevent device system and applications achieving and maintaining optimum security.

Without secure apps and operating system, RN6 and the personal device are suitable targets and inadequate guardianship may facilitate convergence. An employee like RN6 may be the weak link in the organisation's security structure (Colwill, 2009; Verizon, 2019) thus in the context of **RQ1 actual/perceived risks**, devices routinely placed in position of suitable target brought into the workplace may be an actual risk. In respect to **RQ2 average usage/impact**, users may knowingly or unwittingly place themselves in position of suitable target despite limited guardianship in place. A device may have no protection against an

instrument-in-technique with capacity to exploit a vulnerable application, and thus the compromised device may threaten the network.

8.4.4 Summary of Apps and Security in Relation to the Research Questions

Applications are a fundamental element of personal technologies, but security risks are present on many levels. Deficient code can contain vulnerabilities which place a device at risk when taking part in internet activity, malware may be disguised as legitimate services or developers may withdraw support leaving the app unprotected. Users can enable basic device guardianship by installing updates to resolve security flaws and errors or by using antivirus solutions, but findings show that some respondents do not commit to device security. A user with a minimum quantity of self-selected apps may not recognise the importance of regular device and system maintenance. A small number of carefully curated applications may indicate apps of value to the user and suggest that updates are avoided to prevent changes or altered service. In contrast, a user with numerous apps making frequent downloads has increased chance of encountering malware in disguise. Additionally, outdated apps may be concealed amongst multiple icons on a small screen. Neglecting to install an update may imply lack of awareness of the importance of doing so, an indifference to device security or an unwillingness to impair performance. In the context of **RQ1 actual/perceived risks**, an employee without basic guardianship may constitute an actual risk. To conclusively associate actual financial employees with **RQ1 actual/perceived risks** and **RQ2 average usage/impact**, Table 13 (below) illustrates digital activity

taking place regardless of limited guardianship using a small sample drawn from Group C.

	Updates	Anti-Virus	Social media	Games	Streams	Casinos	Adult Content	WhatsApp etc	Dating
RN 6	Sometimes	No	x	x	x	x	x	x	x
RN 17	Sometimes	No	x	x	x			x	
RN 40	Sometimes	No	x		x			x	x
RN 61	Sometimes	No	x		x	x	x	x	x

Table 13. Routine Activity with Limited Guardianship

Using the respondent numbers (RNs) in Table 13 (above) to theorise an example, four employees in a single organisation displaying similar traits may constitute a considerable risk to the IT network. Alternatively, each employee may represent a separate enterprise, hence four corporations might be endangered by behaviours of a single member of staff.

8.5 The Most Popular 'Unsafe' Activities

The final sections examining personal technologies in relation to the central investigation will examine activities with the most user engagement and present results representing the complete sample of seventy-six (N=76) respondents. Section 8.6 is devoted to the use of communications apps and this section (8.5) will consider social media.

8.5.1 Social Networks

Wikipedia holds an inventory exceeding one hundred and eighty-six active social networks (Wikipedia, 2020). New additions to the market like TikTok or SnapChat are favoured by younger demographics (Hamilton, 2019) but Facebook, Instagram and Twitter endure as the three most popular social networks for UK

users (Sarson, 2020). Social networks store a vast reservoir of multimedia content and are of value to both open-source investigators and criminals planning social engineering attacks. Chapter Four, 'The Corporate World' and Chapter Five, 'Executive Risk' made extensive use of social networks as investigation resources and documented how digital footprints may be misused by a threat actor to gather intelligence.

8.5.2 Profiles

The sample were asked to indicate which (if any) social networks they use. Options were Facebook, Twitter or Instagram and no free text option was provided to name any other social network. Figure 30 (below) represents data from seventy-two (N=72) participants.

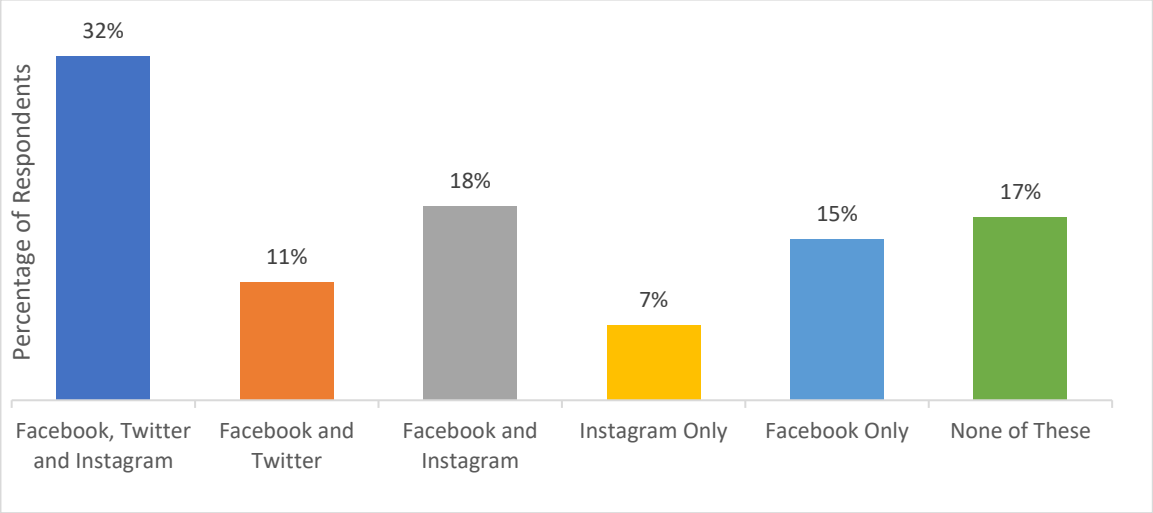

Figure 30. Social Media Profiles

Figure 30 (above) shows that thirty-two percent maintain a profile page on all three social networks. The seventeen percent without a profile on any of the offered platforms were filtered out of the remaining questions.

8.5.3 Social Media Habits

Participants were asked how frequently specific social media activity takes place. The activities have capacity to introduce harms ranging from annoyances such as pop-up advertising to serious threats designed to corrupt a device and are relevant to both **RQ1 actual/perceived risks** and **RQ2 average usage/impact**. The percentage of respondents from a sample of sixty (N=60) is illustrated in Table 14 (below).

	How often do you do the following on Social Media	Always	Quite Often	Sometimes	Very Rarely	Never
a.	Use personal information on a profile page e.g. nickname, occupation, hometown etc	2%	7%	30%	25%	37%
b.	Respond to a private message from a stranger			2%	25%	73%
c.	Click on a link shared by someone outside your network, because the content is appealing		3%	19%	27%	51%
d.	Click on a link shared by a friend to view sensationalist or trending content	3%	8%	27%	37%	25%
e.	Provide a personal email address to receive a free gift or win a prize			8%	17%	75%
f.	Follow a link which claims to reveal who has been viewing your profile			5%	13%	82%
g.	Accept a friend request from someone you don't know or recognise		2%	7%	23%	68%
h.	Click a link promising a free giftcard or prize			7%	17%	77%

Table 14. Respondents and Routine Social Media Activities

Table 14 (above) illustrates specific actions which may initiate suitable target and facilitate possible convergence with an offender or instrument. The results show that the greater number of respondents would 'never' engage in unsafe behaviours. Nonetheless, activities (a), (c), (d) and (g) are of interest. A social engineering attack may commence with a friend request sent to a prospective target and nine percent of respondents stated that they 'Quite Often' or 'Sometimes' accept an unsolicited request from someone outside their network

(g). To convince a target of credibility, an attacker may exploit personal data found on social media profiles. Thirty-nine percent confirmed that they 'Always', ' Quite Often', and 'Sometimes' use personal information on a profile page (a). This may be customary behaviour for some social media users, but as was established in the methodology chapters, this type of active footprint may be exploited in social engineering attacks.

Attackers are known to spread malicious code disguised as a sensationalist, celebrity or human-interest material (O'Donnell, 2020) and twenty-two percent admitted appealing content would be 'Quite Often' or 'Sometimes' accessed by clicking a link shared by an unknown user (c). Thirty-eight percent stated they would 'Always', 'Quite Often' or 'Sometimes' access sensationalist or trending content if it appeared to be sent by a friend (d). Attackers use compromised or 'hacked' profiles to spread malicious material knowing that the content is likely to be accessed because the target believes the "source is legitimate" (Seyler, Li and Zhai, 2020).

8.5.4 Privacy Controls

Respondents were asked whether privacy controls were enabled on social media profiles. Fifty-nine (N=59) participants are illustrated in Table 15 (below).

	Always	Quite Often	Sometimes	Very Rarely	Never
Privacy controls enabled on Social Media profiles	46%	40%	13%	1%	0%

Table 15. Enabled Privacy Controls

Table 15 (above) illustrates that forty-six percent of respondents protect their profile from unsolicited viewing, but fifty-four percent are not consistent with

privacy controls. This has relevance to **RQ1 actual/perceived risks**, particularly when associated with the results seen in Table 14 (8.5.3) where activity (a) indicated that thirty-nine percent of users place personal information on their profile pages. A publicly accessible profile containing personal data may place an employee in position of suitable target for social engineering and is an actual risk.

8.5.5 Work Colleagues as Social Media Friends

Respondents were asked if they would accept work colleagues as friends on social media. Table 16 (below) illustrates a sample of fifty-nine (N=59).

	Always	Quite Often	Sometimes	Very Rarely	Never
Work colleagues as friends or followers on Social Media	17%	32%	34%	15%	2%

Table 16. Work Colleagues as Friends and Followers

Table 16 (above) illustrates that forty-nine percent of respondents will 'Always' or 'Quite Often' accept work colleagues as friends on social media. This may impact upon the privacy of a social media account and be a contributory factor in enabling or instigating social engineering. The relevance of social media colleagues is discussed in detail in 9.4.2.

8.5.6 Frequency of Posting Content on Social Media

PQ61 asked respondents to indicate how often they post specific content to social media. Table 17 (below) illustrates percentages from sixty (N=60) respondents.

	How often is this content posted to social media profiles?	Always	Quite Often	Sometimes	Very Rarely	Never
a.	Self Portraits (selfies)	3%	15%	35%	40%	7%
b.	Photos of spouse or partner		15%	23%	35%	27%
c.	Photos of (your) children		10%	15%	15%	59%
d.	Photos of family (parents, siblings etc)	2%	8%	25%	30%	35%
e.	Comments about spouse or partner		12%	15%	36%	37%
f.	Comments about (your) children	2%	8%	13%	20%	57%
g.	Comments about family (parents, siblings etc)		7%	22%	37%	35%
h.	Comments about friends		23%	43%	25%	8%
i.	Comments about personal hobbies and interests	5%	18%	40%	27%	10%

Table 17. Social Media Content and Frequency of Posts

The content illustrated in Table 17(above) was selected for the contribution it makes to open-source intelligence and the possible benefit to an attacker following a social engineering framework to generate a target profile. Table 17 demonstrates that contributors who affirmed 'Always', 'Quite Often' and 'Sometimes', outnumber those who answered 'Never' in all categories except those relating to children (c) and (f). Category (c) showed that twenty-five percent would 'Quite Often' or 'Sometimes' post photographs of their children, but fifty-nine percent stated they would 'Never' do so. In category (f), twenty-three percent 'Always', 'Quite Often' or 'Sometimes' make comments about their children and fifty-seven percent stated 'Never'. A remark was left by RN40 to say that having neither spouse nor children prevented posting of content regarding immediate family. This respondent was from the 18-24 age group, the largest demographic in the sample. If many younger respondents have no children nor spouse, this may explain the significantly higher percentages of 'Never' in categories (c) and (f). Table 17 additionally demonstrates that fifty-three percent 'Always', 'Quite

Often' or 'Sometimes' post 'selfies' to social media profiles. This is discussed further in Chapter Nine (9.4.5) in the context of 'narcissistic' users and significance to **RQ1 actual/perceived risks** and **RQ2 average usage/impact**.

8.5.7 Social Media in the Corporate Workplace

Figure 31 (below) illustrates results produced by asking respondents how often they use personal devices to conduct social networking in the workplace.

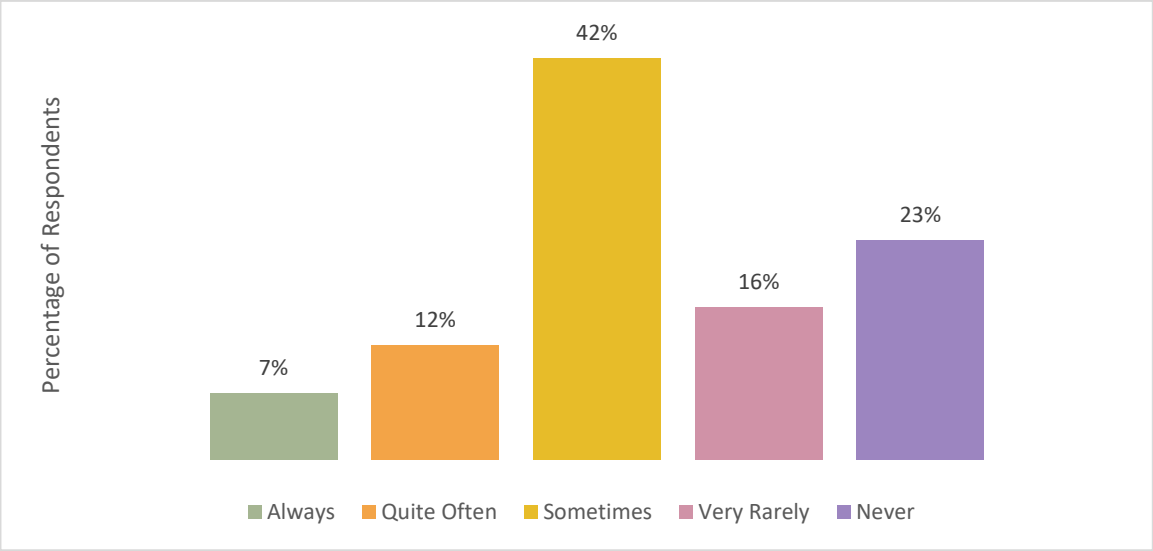

Figure 31. Using Devices for Social Media at Work

Figure 31 (above) illustrates that sixty-one percent will 'Always', 'Quite Often' and 'Sometimes' use personal devices to access social media in the workplace. For the purposes of **RQ2 average usage/impact**, social networks may be used to share scams, hoaxes and malware (see 3.4.3) and a prolific user accessing multiple networks with a personal device has greater potential to converge with offender or instrument-in-technique. Eighty-six percent of the total sample enjoy social networking as a routine digital activity and regular access to social media in the workplace may indicate an avid user. Thirty-two percent of respondents have a profile on three social networks (see Table 30 in 8.5.2) and in the context of

RQ1 actual/perceived risks, employees with a significant online presence may be an actual risk to an organisation. User-generated content and active digital footprints can contribute to targeted social engineering attacks such as spear phishing (see 3.4.1).

8.5.8 Summary of Social Media in Relation to RQ1 and RQ2

The research instrument queried Facebook, Instagram and Twitter and thirty-two percent confirmed a profile on all three. These popular platforms have experienced exploitation as attack vectors to spread malware (Abrams, 2019; Ackerman, 2019; Whittacker, 2018). Thus, users routinely accessing multiple profiles may reinforce position as suitable target and exacerbate capacity for convergence with offender or instrument. Potential for harm may be aggravated by social media use in private space as access is unlimited and activity has no constraints. Unsafe actions may only be prevented by personal guardianship as cyber awareness or device security. Hence, in respect of **RQ1 actual/perceived risks**, an employee who is a prolific user of social networks may represent an actual risk to an organisation and social media might be considered as an attack vector requiring additional security.

The literature evidences that one-in-five organisations has experienced harm due to social media use in the corporate environment (McGuire, 2019) and sixty-one percent of respondents affirmed using social networks in the workplace (Figure 31, 8.5.6). A user may continue with activity begun in personal space, and either disregard any potential risk or assume that corporate security systems will provide protection to the network. Access to social media may be constrained by limited time or presence of senior staff and a ‘quick peek’ may prevent the user from

exercising due diligence towards caution and personal safety. In the context of **RQ2 average usage/impact**, a potential impact to financial systems was demonstrated by eighty-seven percent of Group C who access social media in the workplace, using devices connected to the network (Figure 28, 8.3.2).

Criminals who misuse social media as an attack vector exploit the facilities of the platform to spread malicious content via networks, achieved by abusing trust between users when sharing personal material (Sood and Enbody, 2011). The sample demonstrated that they regularly post content ideal for social engineering, and in particular spear phishing which can target one or more victim with a tailored attack. Contemporary cyber security literature depicts spear phishing as a means to gather intelligence and a principal attack method utilised by cyber-criminal groups (Symantec, 2019, p. 49). In respect of **RQ1 actual/perceived risks**, an *actual* risk may be posed by employees oversharing exploitable personal content which might grant access to a target.

A failure to apply privacy enhancing technologies (PET) to profile pages may exacerbate the possibility of social engineering and inconsistency in use of privacy controls is evident in over fifty percent of the sample. This may be a deliberate decision by the user, or a change or update made by a social platform may result in a once protected profile losing elements of privacy and become accessible without the user being aware. Alternatively, controls may not have been activated when a profile was established, and the user has no opportunity or motivation to return to the settings and enable security. In respect of **RQ1 actual/perceived risks**, prolific users who cannot demonstrate diligence to

protect personal information on all publicly accessible profiles may constitute an *actual* risk.

Social media is a routine activity for most of the sample with eighty-three percent maintaining one or more profiles on three popular platforms. Respondents were not questioned about profiles on lesser known, niche or newer networks; therefore, it is plausible that employees additionally maintain profile pages on other social platforms and may be accessing them in the workplace using a mobile device. In regard to **RQ2 average usage/impact**, the ready availability of a method of access may enable users to consistently increase the quantity of user-generated content which might be used to endanger the corporation. Moreover, frequent access to multiple accounts increases the opportunity for convergence with an attacker or instrument-of-reach.

As Chapter Five, 'Executive Risk' established LinkedIn as an integral resource for detecting executive personnel at risk of targeted spear phishing attacks, a thorough exploration of how respondents engage with the platform took place. Seventy-two percent of respondents maintain a profile on LinkedIn and analysis of the results in association with the research questions can be found in Appendix F. The discussion chapter (Chapter Nine) offers a further evaluation of respondent use of social media, available at 9.4.

8.6 Communication Apps

To continue with the central investigation evaluating actual risk and employee use of personal technologies, it is necessary to examine the possibility for harm to be passed from one device to another. In these circumstances, the threat does not

come from unsafe internet activity but is a deliberate attack designed to exploit vulnerabilities in operating systems or applications. The use of communication apps (also known as instant messaging or chat apps) for example, WhatsApp and Facebook Messenger is widespread amongst respondents. The results of this evaluation may identify whether the use of communication apps is an issue of concern for risk managers.

8.6.1 Routine Use of Communication Apps in Personal Space

Figure 32 (below) demonstrates that ninety-six percent of the overall sample of seventy-six (N=76) routinely use devices to access communication apps in their personal space. The remaining four percent of respondents do not use any communications applications.

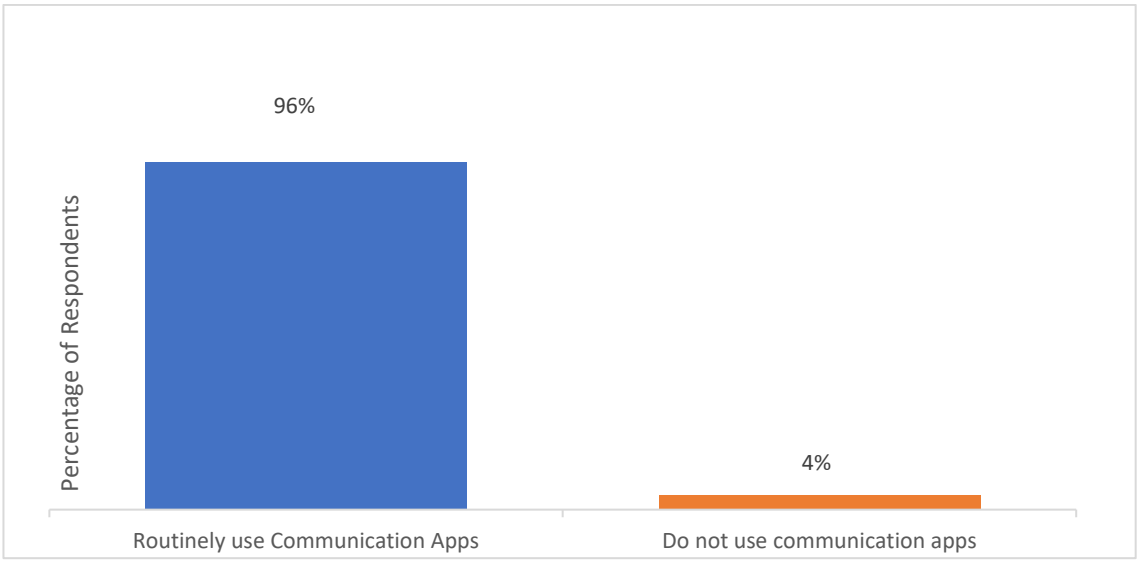

Figure 32. Routine Use of Communication Apps in Personal Space

8.6.2 Quantity of Communications Apps on Devices

Respondents were invited to indicate the quantity of communication apps installed to devices and were asked to select from WhatsApp, SnapChat, Facebook

Messenger, Blackberry Messenger and Yahoo Messenger. Two respondents used the free text field to state that they additionally use Signal. Four people passed the question hence the sample illustrated in Figure 33 (below) consists of seventy-two (N=72) respondents.

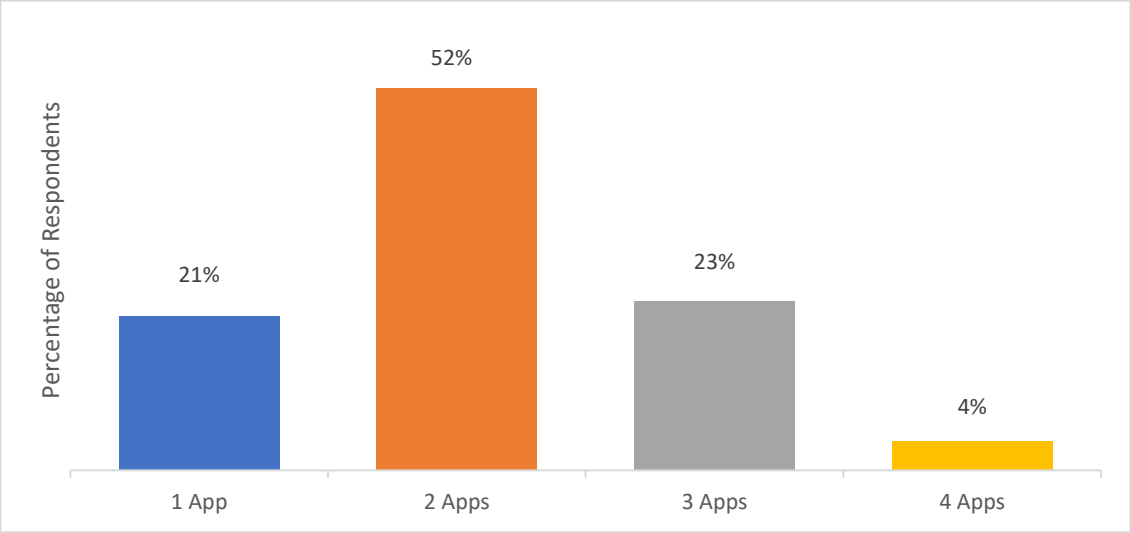

Figure 33. Quantity of Communication Apps on Devices

Figure 33 (above) demonstrates that fifty-two percent have two apps and twenty-three percent have three. Four percent of the sample have four communications apps on their devices. A further four percent of the sample asserted that no communications apps were installed and are not included in the results seen in Figure 33.

8.6.3 Popular Apps

Figure 34 (below) illustrates the percentage of respondents using popular communications applications. The sample is sixty-nine (N=69).

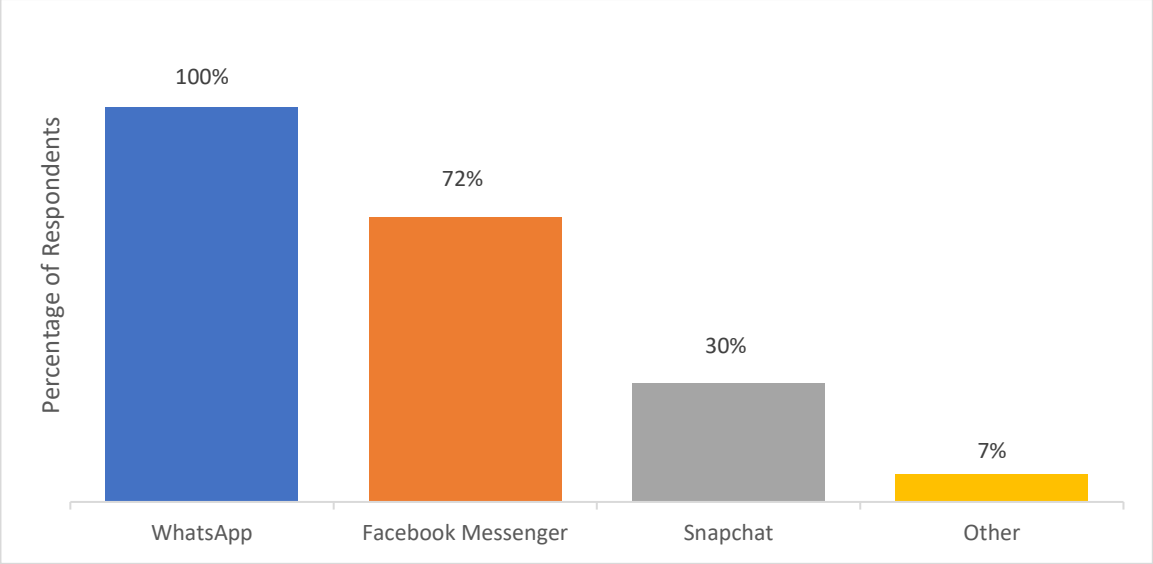

Figure 34. Popular Communication Apps

Figure 34 (above) illustrates that the most popular choice is WhatsApp, and one hundred percent have this application installed to a personal device. Seventy-two percent have Facebook Messenger and thirty percent have Snapchat. Results for Snapchat deviate from the literature which proposes that eighteen to twenty-four is the predominant age demographic of UK Snapchat users (Influencer Marketing Hub, 2019), but only one respondent came from this user group. Instead, nineteen percent of Snapchat users are aged twenty-five to thirty-five and ten percent are thirty-five to forty. The Snapchat sample conforms with the literature regarding predominant user gender as twenty percent of the sample are female (Clement, 2020d).

8.6.4 Communication Apps used in the Workplace

Respondents were asked if they would access and use a communication app whilst at work. Figure 35 (below) illustrates a sample of sixty-nine (N=69).

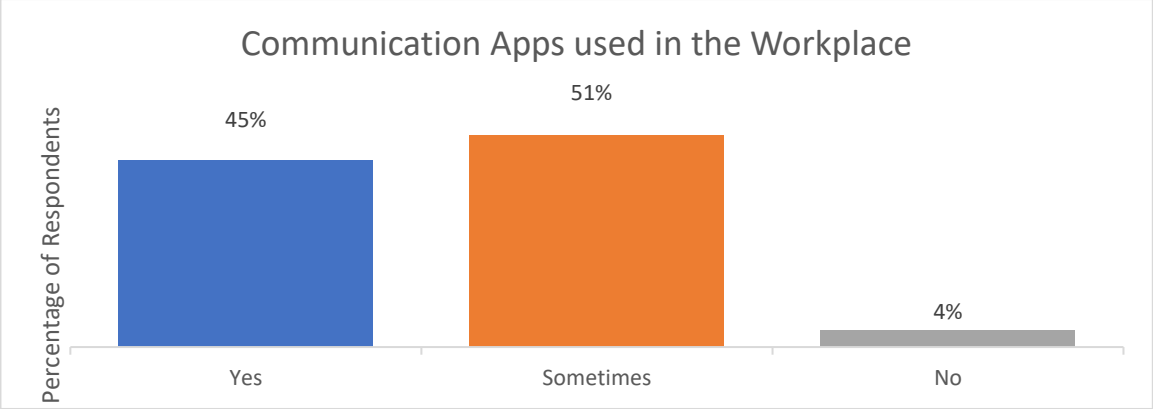

Figure 35. Communication Apps used in the Workplace

Figure 35 (above) shows that ninety-six percent of the sample 'Always' or 'Sometimes' use communications apps at work. Only four percent of the sample stated that they do not. WhatsApp is (apparently) particularly vulnerable to elaborate strategies designed to dupe users into sharing or downloading malware (Anstett, 2019; Cuthbertson, 2019b) (see 7.4.7). This may be due to popularity of the application and the recognised strategy of attackers choosing to target software with the greatest number of users. One hundred percent of respondents confirmed that WhatsApp is downloaded to their device (see Figure 34, 8.6.3). This known attack vector is being accessed by employees in the financial workplace and is relevant to **RQ2 average usage/impac**t.

8.6.5 Summary of Communications Apps in Relation to RQ1 and RQ2

Communications apps use Wi-Fi or mobile data to enable 'chat' with other users using text-based messages or video calls. Images, video and hyperlinks to web-based content can be sent to one or multiple users and WhatsApp and Facebook Messenger can send and receive PDF, Word, and Excel documents and spreadsheets. Recent statistics indicate that WhatsApp has two billion global users and Facebook Messenger has one point 3 billion (Bucher, 2020). The

popularity of web-based messaging is reflected in the results as twenty-seven percent of respondents have a minimum of three applications on their devices, and fifty-two percent use two messaging services.

Communication applications are regularly reported to be vulnerable to attackers. Malware, fraud and other threats can be shared (Blanco, 2020) and scam messages can be doctored to appear to come from legitimate organisations (Which, 2020). Security flaws have been identified in WhatsApp, which could enable attackers to manipulate personal content and “corporate documents” (Amit and Gat, 2019, para. 1). Malicious code can be hidden in specially created images and activated when the user opens the picture (CisoMag, 2020). A vulnerability in WhatsApp has been used to install malware by a single phone call (Lee, 2019; Newman, 2019a; WhatsApp, 2020). Snapchat is a vehicle for scams and phishing (Dassanayake, 2019; Martin, 2018). Vulnerabilities have been found in the WhatsApp desktop application which might “aid phishing campaigns, spread malware and potentially even ransomware” (Safruti, 2020, para. 1). Thus, employees who download WhatsApp to a company laptop or PC may unwittingly infect a device connected to the network with malware. In respect of **RQ1 actual/perceived risks**, employee use of communications and instant messaging in the workplace may constitute an actual risk.

In the context of **RQ2 average usage/impact**, devices compromised by a successful attack against a communications application may not necessarily require legitimate access to the corporate network to spread the exploit further. A simple action such as charging a smartphone by connecting it to a laptop or

desktop PC with a USB cable may be adequate to spread malware (Krug, 2019). The use of WhatsApp, Facebook Messenger and Snapchat in the personal space may constitute a risk which might threaten the network if the device is later brought into the workplace. Additionally, use of messaging apps in the workplace may "undermine corporate network security" and enable access to corporate systems for malicious actors (Dungay, 2019, para. 3). Further discussion about communication applications can be found in 9.3.2.

This section concludes analysis of the data concerning mobile devices. Themes and issues identified in the results will be discussed further in Chapter Nine. The remainder of Chapter Eight is devoted to the Internet of Things and **RQ3 IoT unexplored risk** and will commence with a brief overview of smart technologies before introducing the results extracted from respondent data.

8.7 The Internet of Things (RQ3 IoT unexplored risk)

The analysis thus far has favoured Research Questions One and Two and theorised how routine activity may position a user, device or organisation as suitable target. **RQ3 IoT unexplored risk** will now expand the evaluation to include 'smart' consumer devices as personal technologies. The 'Internet of Things' (IoT) describes objects which collect, analyse and share real-time data using the internet and can include inanimate items or living creatures (Vyas, Shukla and Doshi, 2019). The varying technologies necessary to implement the IoT present exclusive dilemmas and challenge the use of traditional security solutions (Radoglou et al., 2019). Quandaries include vulnerabilities in software, hardware or supporting infrastructure (Miessler et al., 2019), IoT specific malware

(Alasmary et al., 2019) and applying robust security to low-cost devices with limited processing capacity (Safaei Pour et al., 2019). The IoT predicament is exacerbated by a lack of robust leadership in respect to managing security risks, and no employee training or awareness raising (Ponemon Institute, 2019).

Home systems, appliances and wearables were introduced as consumer IoT in 3.11 and applicable respondents were surveyed about smart device ownership and IoT command-and-control apps installed to personal devices. Section 8.7 begins by recording the relevant results and is followed by a focused analysis of IoT users to theorise where risk may arise. Themes will be compared with trends observed in contemporary literature to suggest current and future issues which may interest security managers. As in the previous sections, the sample size will vary throughout the narrative and charts and tables will illustrate either percentage of the dataset or number of respondents as appropriate. To differentiate between various categories of consumer IoT, the term 'IoT unit' will refer to a home-based system or appliance. A 'wearable' will describe any device worn on the body, for example a watch, fitness tracker, medical device, item of clothing or footwear. Where necessary, descriptive text will provide further information. Observations of relevance to the central investigation, limitations in the data and inconsistencies in the survey logic will be addressed in Chapter Nine or the appendices. The reader will be directed accordingly.

8.7.1 Employee IoT

The IoT section of the research instrument presented respondents with a list of appliances, home systems and wearable devices and asked them to indicate whether they possessed any personal IoT. Four respondents passed the question, nineteen answered negative and were filtered to the next applicable part of the survey. Figure 36 (below) shows results for fifty-three (N=53) participants.

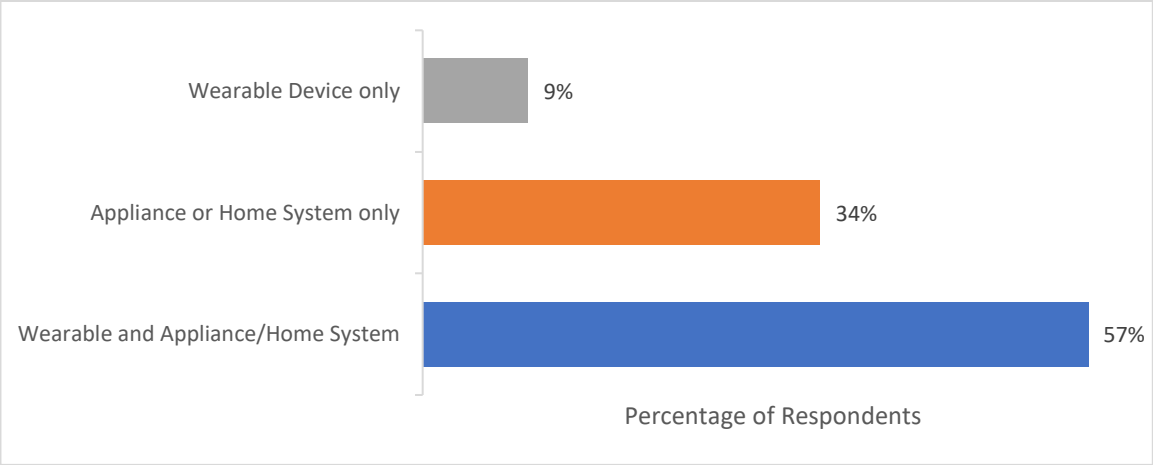

Figure 36. Employee IoT

Figure 36 (above) demonstrates that more than half the dataset (fifty-seven percent) owns a wearable device in addition to either an appliance or home system. Thirty-four percent have either a home system consisting of several connected elements, or a voice activated assistant. Only nine percent of the sample own a wearable device with no other investment in IoT.

8.7.2 Category of IoT

Respondents were asked to specify the category of consumer IoT. Manufacturers and brands were irrelevant. Figure 37 (below) shows the percentage of respondents owning each type of each unit. Sample size is fifty-three (N=53). Music systems and virtual assistants are the most widespread appliances and systems items. Fitness

trackers are the most prevalent wearable device. Other types of wearables are a health monitor, footwear and a GPS watch. Home environment and security systems are popular, but appliances are more common than systems for home surveillance. Three participants used free text to state that their appliances are smart television sets and a kettle.

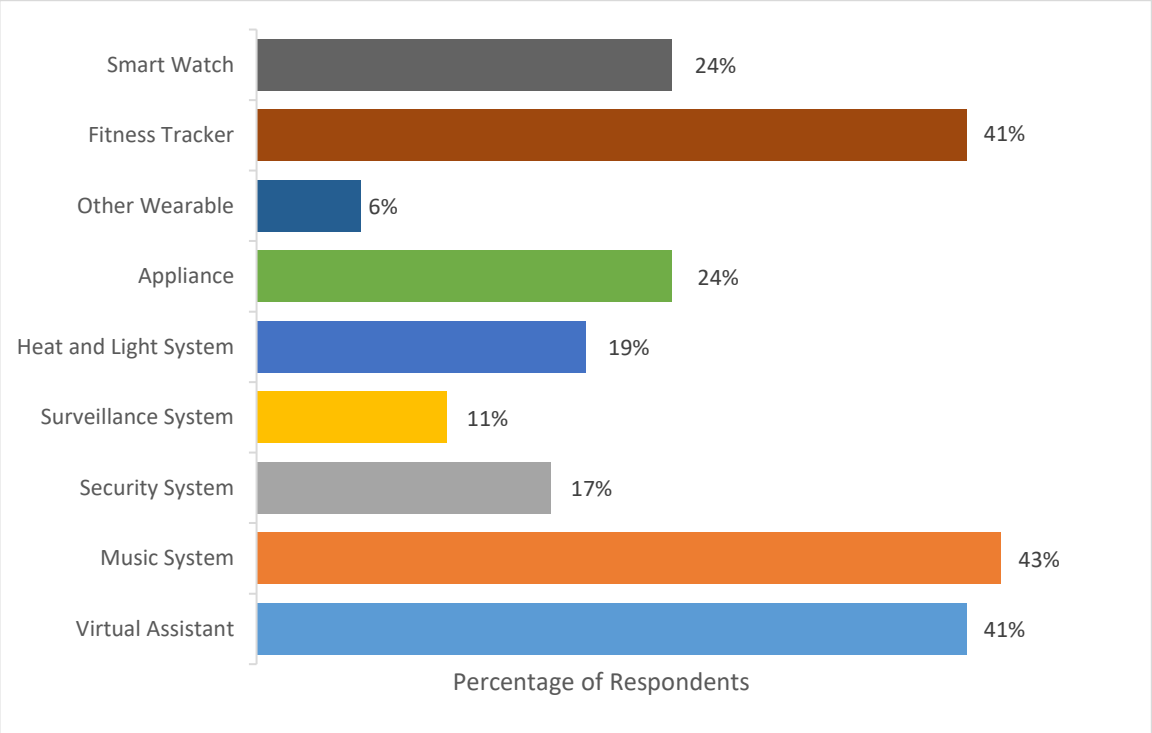

Figure 37. Category of IoT

8.7.3 Quantity of IoT Units Owned by Employees

Figure 38 (below) illustrates the percentage of respondents owning specific amounts of IoT. Sample size is fifty-three (N=53). Thirty-two percent own a home system or appliance in addition to a wearable device, generally a fitness tracker or smartwatch. Six percent of users own two wearables in addition to other IoT appliances or home-based units. For example, RN38 has a fitness tracker and health monitor, RN9 has a fitness tracker and smart watch.

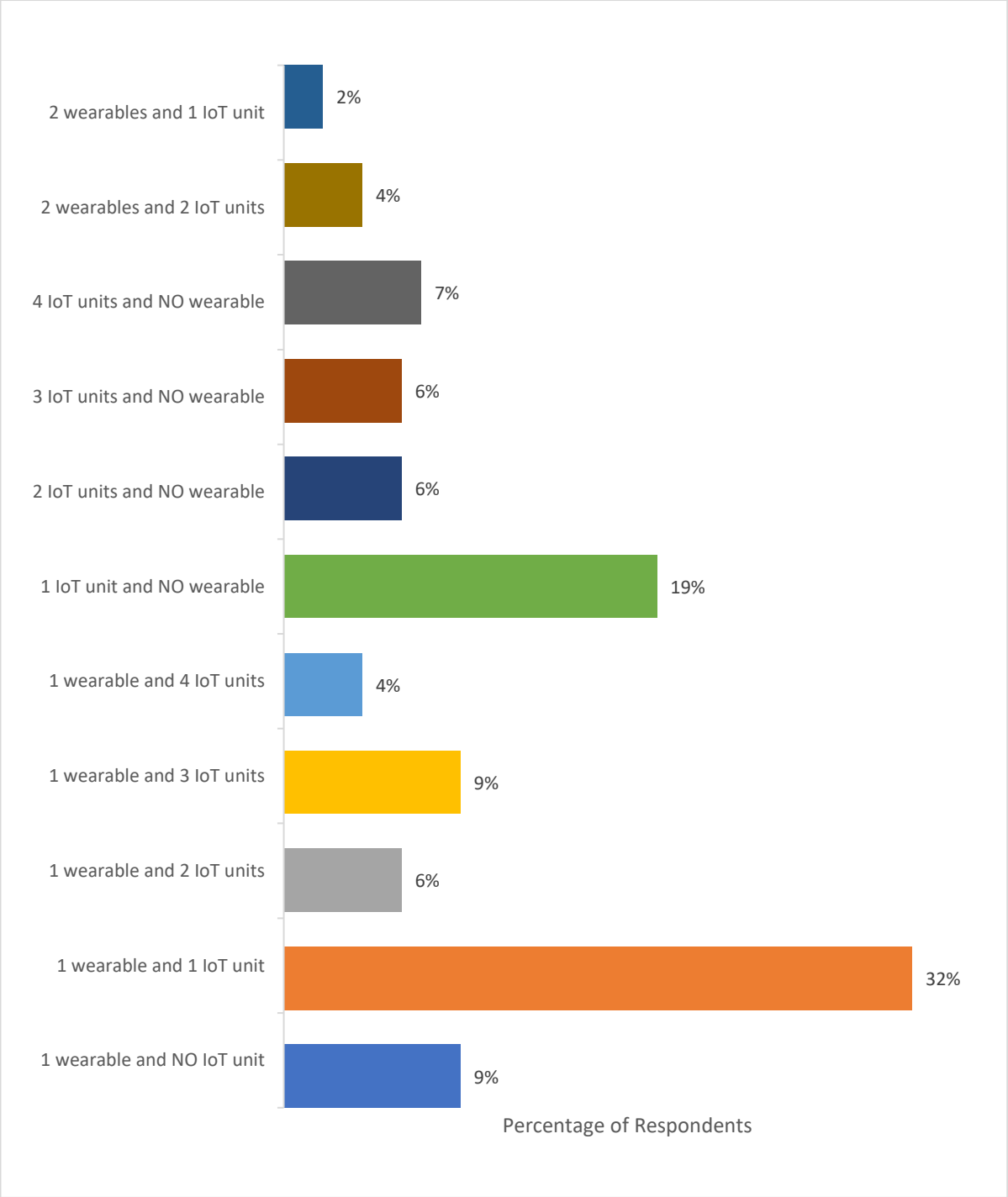

Figure 38. Quantity of Employee-Owned IoT

8.7.4 IoT Combinations

The results suggest that users embracing smart technologies possess more than one home system or appliance. Table 18 (below) shows a small sample of IoT combinations and illustrates that enthusiastic users are combining environmental and safety systems with music systems, appliances and wearables.

RN	IoT DEVICES				
RN18	Virtual Assistant	Music System	Heat and Light	Surveillance System	Smart Watch
RN24	Virtual Assistant	Appliance	Heat and Light	Smart Watch	
RN30	Music System	Security system	Heat and Light	Appliance	
RN33	Virtual Assistant	Security system	Appliance	Surveillance System	Smart Watch
RN34	Virtual Assistant	Music System	Appliance	Smart Watch	
RN38	Surveillance System	Security system	Fitness Tracker	Health Monitor	

Table 18. Combinations of Consumer IoT

8.7.5 Device Security

The samples illustrated in the remainder of Chapter Eight vary in size as some respondents chose not to provide data. PQ57 enquired whether participants had researched the in-built security for their chosen device prior to making a purchase. Those who did not conduct security research were subsequently asked to select a reason for not doing so. A free text option accompanied both questions for respondents to comment on their decision-making. Figure 39 (below) illustrates the percentage of users from a sample of thirty-six (N=36) who considered device security a factor in their choice of purchase.

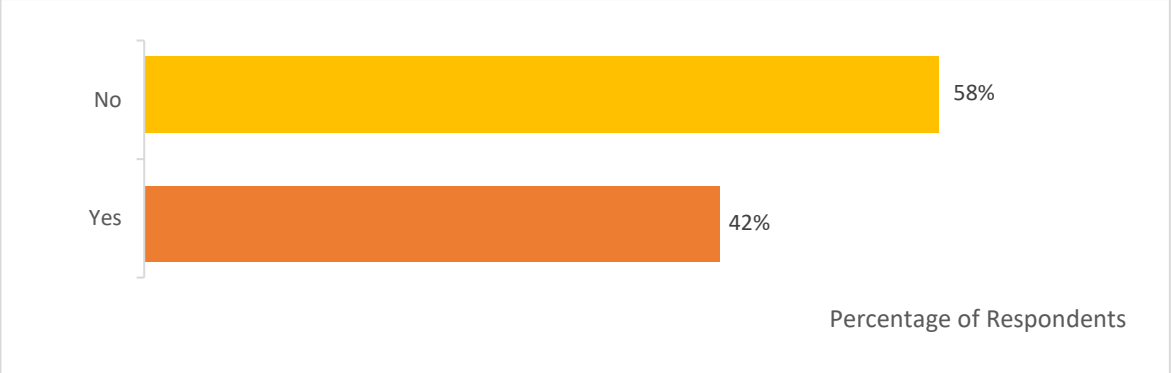

Figure 39. Security Research Prior to Purchase

Figure 39 (above) illustrates that forty-two percent considered security as important and conducted research prior to making a purchase. RN20 commented that the research caused subsequent avoidance of a particular brand as security had proved inadequate. Fifty-eight percent represents the users who acquired IoT with no prior knowledge of security mechanisms built into the device. RN2 reported that no research was conducted as the device was purchased from a reputable provider, implying that users may consider a brand name as sufficient guarantee of a quality product.

Respondents who did not conduct security research were invited to indicate why they had not done so. Figure 40 (below) represents a sample of twenty (N=20).

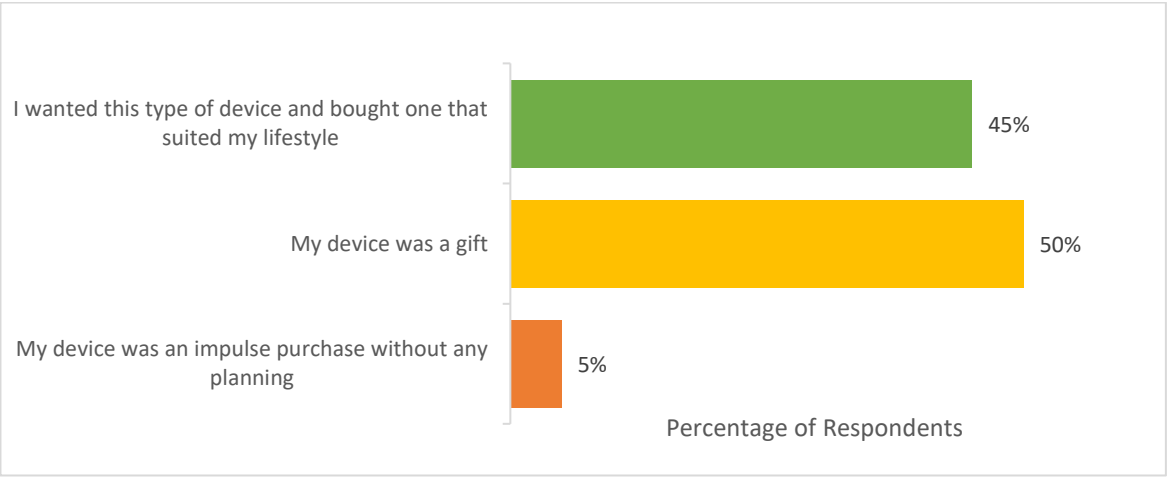

Figure 40. Reasons for No Security Research

Figure 40 (above) illustrates that forty-five percent did no research because they desired a particular device to suit their lifestyle. These results appear consistent with literature suggesting that consumers are complacent about seeking security information (Harris Interactive, 2019). RN19 added a comment to say, “I simply had not even considered I needed to think about security for Wi-Fi music device. I am now wondering whether I should do?”. This statement may indicate minimal user comprehension regarding IoT security, perhaps due to assumption that robust solutions are already present. An (apparent) lack of security knowledge has relevance to **RQ3 IoT unexplored risk**. Fifty percent claimed that no security research took place as devices had been gifts and they had no control over provider, nor quality of device and again is relevant to **RQ3 IoT unexplored risk**.

8.7.6 Updates to IoT Devices

PQ58 asked respondents how they respond when advised by the manufacturer to download an update for their IoT device. Figure 41 (below) illustrates results from a sample of twenty-six (N=26).

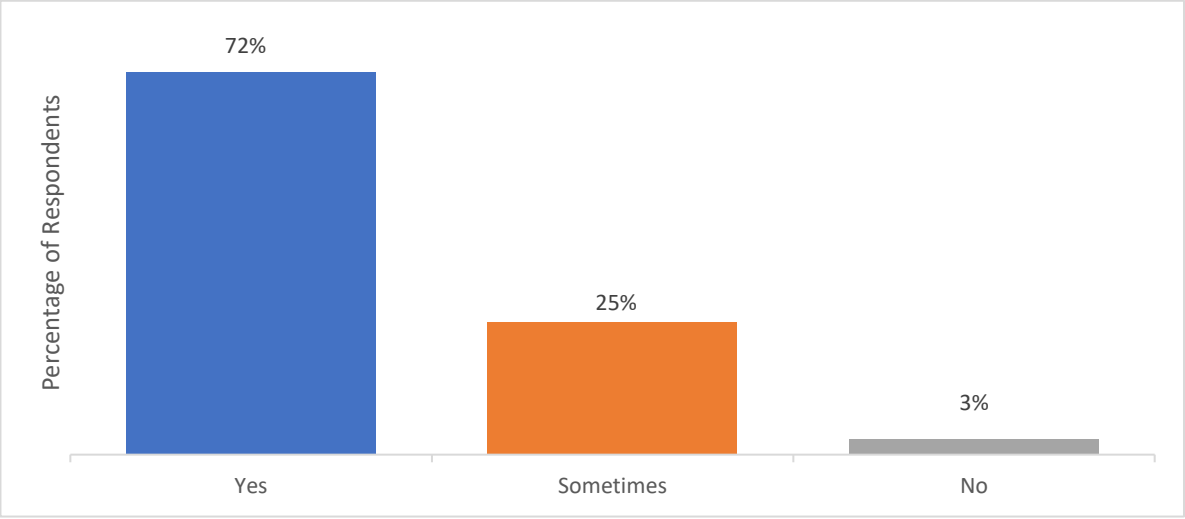

Figure 41. Install IoT Updates

Figure 41 (above) illustrates that seventy-two percent update their devices when prompted, but three percent never do. Twenty-five percent are inconsistent with updates, and fourteen percent of these are from the dataset who made no investigation of device security. The literature implies that users assume “security features are already built into devices” particularly those from established providers (Harris Interactive, 2019, p. 3; Minister for Digital and Broadband, 2020, p. 6). Thus, this group may have no awareness of software vulnerabilities and necessary updates to repair them, assuming instead that manufacturers have made devices secure in production. This potential lack of awareness has significance for **RQ3 IoT unexplored risk**. Eight percent of those who ‘Sometimes’ update is from the group who had conducted security research prior to purchase. Having investigated security mechanisms it might be assumed that consumers would ensure they were implemented. The findings suggest that device owners are unaware that security can only be maintained by responding to any prompt to update the device or application.

Four respondents who received IoT as gifts were amongst those who ‘Sometimes’ install updates. These users may have had no influence over brand or safety features and devices with already inferior security may not be receiving regular updates. A further concern is that those who receive gifts may not have chosen to acquire IoT, due to lack of interest in the technology. The importance of updates may not be fully recognised and without enthusiasm for the device a user may not endeavour to maintain it, thus indicating relevance to **RQ3 IoT unexplored risk**.

8.7.7 Default Passwords

Respondents were asked whether the default password supplied with their device was amended when the device was installed. Six people passed the question and Figure 42 (below) consists of forty-seven (N=47).

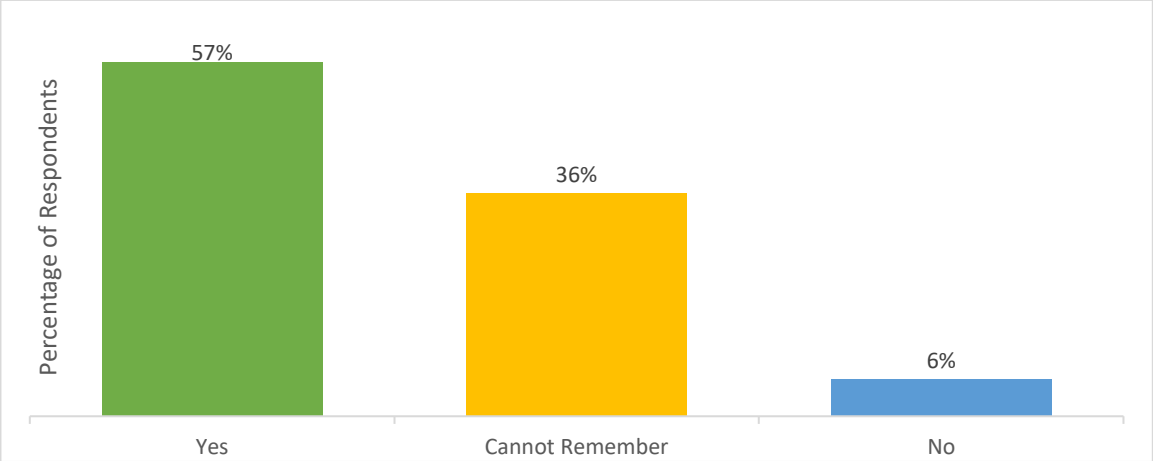

Figure 42. Default Password Changed When Device Installed

Figure 42 (above) illustrates that despite fifty-seven percent confirming a change of default password, thirty-six percent cannot remember, and six percent acknowledge not amending the factory issued version to a secure personal one. As results demonstrated in Figure 37 (8.7.2) showed that many respondents own multiple devices, the 'Cannot Remember' sample was examined further. Figure 43 (below) illustrates the percentage of respondents owning devices which may retain a default password. The sample is seventeen (N=17).

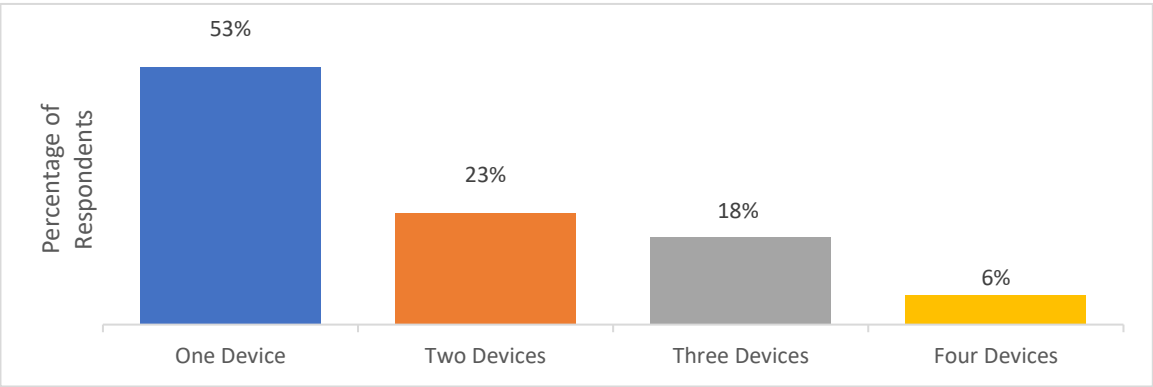

Figure 43. Percentage of Respondents Owning Devices which may Retain Default Passwords

Figure 43 (above) suggests that fifty-three percent of respondents own a single device which may retain the factory password, and six percent own four individual IoT devices which may be unsecure. Default passwords have been identified as vulnerabilities affecting the security of already weak devices (Anderson, 2019; Microsoft, 2019) and the literature discussed the UK legislation implemented to improve security (Minister for Digital and Broadband, 2020) (see 3.11.4). Although not illustrated in these results, the sample of seventeen users seen in Figure 43 own a total of 30 devices. This suggests that a substantial number of IoT devices may be present or represented in the workplace with default passwords as potential entry points into an organisation and subsequently significant to **RQ3 IoT unexplored risk**.

8.8 Consumer IoT in the Workplace

RQ3 (**IoT unexplored risk**) aims to establish whether consumer IoT is present in the workplace and evaluate any potential impact to the corporate IT network. Findings confirm that respondents own a variety of IoT units and wearables, and the next series of results will dissect the dataset of IoT users to explore user behaviours and potential risks. As seen previously, sample size will vary, dependent on observed themes and number of respondents who provide data. The accompanying charts will illustrate the results.

8.8.1 Wearable Devices

The number of wearable devices owned by respondents included twenty-two fitness trackers, thirteen smartwatches, one GPS watch, one health monitor and an item of footwear. Figure 44 (below) illustrates percentage of respondents who wear a device in the workplace. The sample consists of thirty-five (N=35).

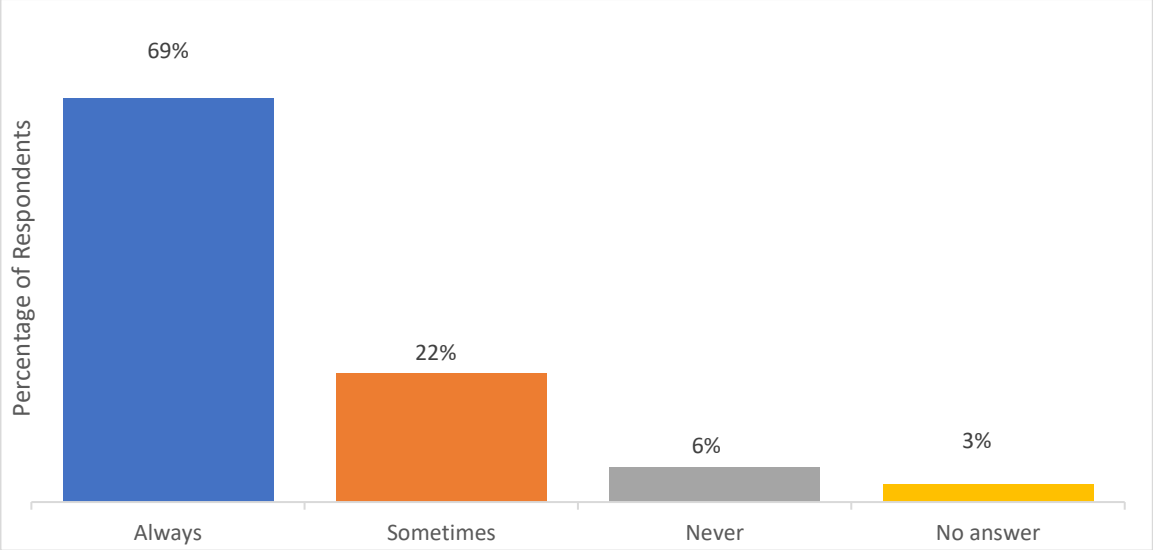

Figure 44. IoT Worn in the Workplace

Figure 44 (above) illustrates that sixty-nine percent 'Always' wear their device in the workplace and twenty-three percent will 'Sometimes'. Only six percent stated that they 'Never' wear their device at work. RN36, who owns the IoT footwear, was the only participant to pass the question.

8.8.2 Wearable Devices Connected to the Network

The dataset who 'Always' and 'Sometimes' wear devices to the workplace were examined to ascertain whether devices were connected to the corporate network. Figure 45 (below) illustrates thirty-two (N=32) respondents.

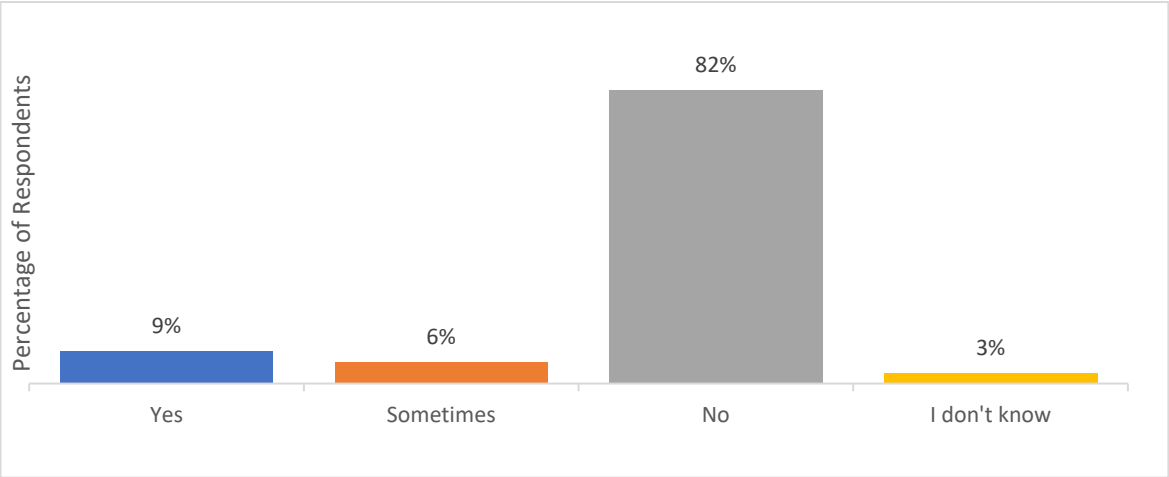

Figure 45. Wearable Devices Connected to the Network

Figure 45 (above) illustrates that the majority (eighty-two percent) of users wearing a device to the workplace do not allow it to connect to the network. Nonetheless, nine percent confirmed that wearables would always connect to corporate Wi-Fi. As these respondents had previously stated that their devices are always present in the workplace, it is possible an automatic connection requiring no user-intervention occurs when the device is in range of the corporate Wi-Fi (Ptsecurity, 2017). Alternatively, each employee may instigate a manual connection on entering the corporate space. All respondents in this sample displayed an aptitude for security, amended default passwords and always install updates. Despite this, small devices and wearables may be an access point into corporation networks due to limited capacity for robust security or poorly configured software (see 3.11). In spite of best attempts at security, the inherent limitations in IoT devices may render users' efforts meaningless. Although the sample is small, the results are relevant to **RQ3 IoT unexplored risk.** Users are connecting wearable devices to the corporate network and possibly introducing an exploitable vulnerability into the workplace.

8.8.3 IoT Applications on a Device Connected to the Network

Group C and routine digital activity using personal devices connected to the corporate network was documented previously in Chapter Eight (8.3 and 8.4). The dataset was revisited for further evaluation to ascertain the presence of IoT command-and-control applications on personal devices. Figure 46 (below) illustrates the number of IoT apps present in Group C. The sample consists of twenty respondents (N=20).

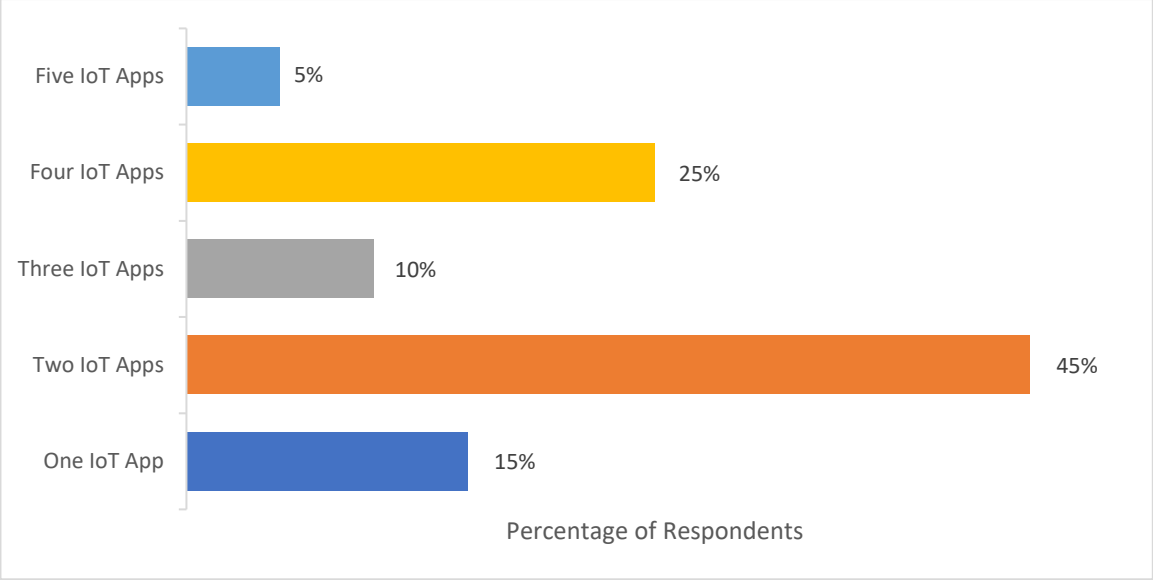

Figure 46. IoT Apps on Devices Connected to the Network

Figure 46 (above) shows that twenty-five percent of Group C have four IoT apps on personal devices controlling home systems, appliances, voice activated assistants or wearable devices. Forty-five percent have two apps. IoT apps are known to have unsecured cloud connections and may contain vulnerabilities in the code (Barcena and Wueest, 2015; Yu et al., 2020). Vulnerabilities in IoT devices can be exploited by IoT-specific malware (Costin and Zaddach, 2018) which may be polymorphic (Darabian et al., 2020) and engineered to defeat traditional detection methods (Drew, Hahsler and Moore, 2017; Masabo et al., 2018 (see 3.3.2). A compromised consumer IoT device accessed via a vulnerable application may infect the mobile device with IoT specific malware. In the context of **RQ3 IoT unexplored risk**, if the device is connected to the corporate network, malware could spread throughout enterprise systems. The small sample of twenty (N=20) from Group C have a combined total of fifty-two IoT applications installed on smartphones which connect to the corporate network. To place this in perspective, a large workforce may have hundreds of IoT apps on devices in the

corporate workspace. If company policy allows connection to the network, corporate assets may be at risk.

8.8.4 IoT Accessed from the Workplace

Thirty-two participants (N=32) provided data when asked if IoT devices are accessed while the user is in the workplace. Sixty-nine percent confirmed access at work, using an application downloaded to their smartphone. This sample was invited to use a free text option to explain why IoT is accessed at work. Eighteen (N=18) participants responded, and Table 19 (below) presents the comments.

RN	Device(s)	I access my IoT at work because.....
RN5	Smartwatch	Read emails and messages.
RN9	Virtual Assistant, Security , Fitness Tracker, Smartwatch	Fitness Tracking.
RN13	Virtual Assistant, Fitness Tracker	Update, play music, log water.
RN14	Surveillance , Fitness Tracker	Occasionally check-In.
RN18	Virtual Assistant, Music , Heat/Light , Surveillance	Sometimes it's necessary.
RN19	Music , Smartwatch	I sometimes use my watch for other things at work, ie messaging, calls etc.
RN24	Virtual Assistant, Heat/Light , Appliance, Smartwatch	To pre-heat my home.
RN26	Music , Heat/Light , Smart TV, Fitness Tracker	To look at activity levels in any given week.
RN32	Virtual Assistant,Music , Fitness Tracker	To check activity progress through the day.
RN33	Virtual Assistant, Surveillance, Security, Appliance, Smart Watch	Notifications on my phone/watch for my home security system.
RN38	Surveillance, Security ,Fitness Tracker, Health Monitor	I am conscious of my surroundings and health.
RN46	Music , Fitness Tracker	To count steps and log food.
RN50	Fitness Tracker	To check step count and heart rate, general fitness.
RN53	Security , Fitness Tracker	To answer the door if the doorbell rings.
RN55	Fitness Tracker	To track my fitness, I train 5 days a week.
RN56	Virtual Assistant, Fitness Tracker	To update lists, add reminders, see how I'm getting on.
RN61	Appliance, Fitness Tracker	To keep track of how much activity I've done during the day.
RN70	Heat/Light , Surveillance , Smartwatch	To keep an eye out when there is someone approaching the house.

Table 19. IoT Accessed in the Workplace

The comments in Table 19 (above) show that respondents access devices which are both physically present in the workplace and virtually represented by an application on the user's smartphone. The facilities of fitness devices and smartwatches are used to update health data or receive reports on personal progress and remote access is used to respond to alerts sent by home security and surveillance systems. In regard to **RQ3 IoT unexplored risk**, IoT devices are established in the workplace both virtually and physically. In respect of potential risk to the network, small devices like wearables may be typical of weak security due to limited capacity for robust security (Bertino and Islam, 2017; Safaei Pour et al., 2019) and applications are unsecured or contain vulnerabilities (Barcena and Wueest, 2015; Yu et al., 2020). Fifty-five percent of respondents represented in Table 19 are accessing IoT apps using smartphones connected to the corporate network. This suggests that consumer IoT in the workplace may be an issue for security managers to address.

8.8.5 Connecting to an Alternate Network

Throughout the analysis, inconsistency has been noted regarding number of devices confirmed to access enterprise networks. Section 8.3 observed that of fifty-one users who conduct workplace activity using personal devices (Group C) only sixty-seven percent access the network. Figure 45 (8.8.2) illustrated that fifteen percent of users wearing an IoT device will connect the device to the network, but eighty-two percent will not. The inconsistency in network connection can be seen amongst specific device users, as an example, four smartwatch wearers connect to corporate Wi-Fi, but nine other smartwatch wearers do not.

The disparity seen in the results suggests that alternate methods of connectivity to access online services may be used in the workplace. Employees may be utilising personal mobile data or corporations might provide an alternative or 'guest' network for the benefit of workers or visitors to corporate premises. Industry experts recommend a separate network for IoT devices to prevent malware or attackers from reaching critical systems (Cimpanu, 2019c; Norton, 2020). A guest network will provide access to the internet and other essential facilities but offer some protection to the corporation (Mitchell, 2019). In the context of the cyber-RAT framework, alternate internet access may be a capable guardian to prevent convergence with offenders. Nevertheless, access to harmful internet content or an unsecured IoT device seeking Wi-Fi connectivity may still compromise a guest network (Slattery, 2018). A poorly configured network (Kinzie, 2019, part 7) or unsecured router (Ovadya et al., 2019) can threaten corporate systems or critical data. Security managers and threat intelligence officers should not consider the use of an alternate network as a failsafe solution. This is particularly relevant for enterprises with no department designated to manage IT infrastructure where responsibility may be delegated to average-user employees without specialist knowledge. Alternative and guest networks were not addressed in the research instrument and the data is therefore limited in respect to theorised and actual risk arising from routine digital activity, personal devices and IoT. A complete discussion relating to guest networks and the limitations can be found in Appendix G.

8.8.6 Summary of IoT Results in Relation to the Research Questions

The IoT survey was designed to query the presence of IoT and associated applications in the financial workspace. The results confirm that employee engagement with consumer IoT is substantial, and respondents possess a variety of IoT systems, appliances and wearables. In the context of **RQ3 IoT unexplored risk**, users who purchase IoT as a lifestyle choice may consider that reputable providers will guarantee security and so do not make personal security investigation prior to purchase. The literature suggests that IoT brought hastily to the consumer market may lack intrinsic safety (Britton, 2016; Carr, 2019; Spiezle, 2016; Verizon, 2015) and novelty devices from small, unknown manufacturers may not have the guarantee of a reputable brand. This may consequently introduce poorly configured devices or applications into the workplace with the potential to threaten the network.

In respect to **RQ1 actual/perceived risks**, employees are expanding the academic framework of insider risk and introducing new technologies which may not be mitigated by conventional workplace policies. Factory set default passwords are of such concern that UK legislation has been amended to address the issue, but IoT owners could not remember changing default passwords and only ‘Sometimes’ apply updates indicating a general lack of IoT awareness or indifference to security. A possible concern is that of IoT received as gifts since receivers of unexpected IoT may have no knowledge of device security, nor be aware of the requirement to install regular updates. The recipient of an impulsive gift may have no vested interest, unlike a consumer eagerly anticipating a ‘smart’ device. Consequently, ‘detached’ users may be wearing devices or using

appliances they did not choose or have no affiliation with, and basic guardians may not be enabled or maintained. A further consideration is that IoT given as gifts may continue to have relevance beyond the new legislation. Global marketplaces will facilitate purchase of devices, systems and appliances from alternate sources other than UK regulated manufacturers, and those receiving gifts will have no control over the origin of a device or system.

The proposed legislation will improve overall IoT security and may thwart future attackers, but results show that IoT is already in the workplace. One hundred and sixteen (116) IoT applications are present on smartphones in corporate space with some devices carrying up to five apps to control various IoT devices. The small sample of fifty-three possess one hundred and twenty-one (121) devices in total. Hence, in large financial corporations with hundreds of employees, there may be thousands of virtual or physical IoT already present in the workplace. In the context of **RQ2 average usage/impact** employees are using personal technologies to access and control IoT from the workplace using corporate network connectivity. To increase security, advisors recommend that IoT devices use an alternate network, but harm may still be introduced by apps or devices and the threat of a compromised guest network still exists. Any weakness in the security of an alternate network caused by incorrect configuration or lack of router maintenance may ultimately allow access to corporate assets and critical data.

8.9 Conclusion to Analysis and Interpretation

Chapter Eight assessed the results with the intention of extracting data relevant to the research questions. Respondents were evaluated using contemporary literature and the cyber-RAT framework, and potentially 'unsafe' digital activity was observed using company-issued devices and personal technologies carried from home to the workplace. Corporate devices may have access to company networks and/or corporate data and in accordance with **RQ1 actual/perceived risks**, use of company property to access social media or download applications may be an actual risk to be addressed by stakeholders. In respect to **RQ2 and average usage/impact**, employees from all levels of corporate hierarchy allow devices used for potentially 'unsafe' personal activity to connect to enterprise IT infrastructure and personal activity may continue whilst in the workplace. In spite of potential for internet harm introduced by application-based services and evidence of significant user-engagement with known attack vectors such as social media and communication apps, basic user guardianship methods are not embraced by all users. Regular updates and antivirus are lacking and reliance on assumed guardianship is evident.

In regard to **RQ3 IoT unexplored risk**, IoT is established as physically present in the financial workplace and significant virtual representation exists in the form of command-and control applications downloaded to employee-owned smartphones. An enthusiasm for IoT is observed in users owning multiple systems, devices and appliances, suggesting potential for further investment in smart technology. This will be discussed further in Chapter Nine in association with emerging trends for connected devices. A lack of concern for IoT security is demonstrated by users

desire for a lifestyle device or receiving IoT as a gift. Results confirm that not all users accept device updates, and passwords may not be modified from the default factory setting, implying a general lack of awareness regarding maintenance of a secure system. These findings relevant to the central investigation will be elaborated further in the discussion in Chapter Nine. Themes drawn from the results will be discussed and the cyber-RAT framework applied as a tool to evaluate average user activity with concept of suitable target and capable guardian to resolve the research questions and offer original contribution.

Chapter Nine: Discussion

9.1 Introduction

The narrative thus far has documented findings which focus on activity indicative of risk to enterprise workspace. Chapter Nine will elaborate on crucial findings, supplemented with insights drawn from the methodology chapters to confirm the literature and offer original contribution. The discussion begins in 9.2 with an examination of observed limitations caused by the research instrument and respondent actions during the survey process. Section 9.3 returns to the results to address key themes relevant to the central research questions and connect them to academic works and contemporary security literature as an aid to identifying threats. Section 9.4 deliberates on social media in association with employee behaviours evidenced in the data. In 9.5, appropriate issues observed in the results are proposed as items to be addressed during bespoke training and awareness. Section 9.6 suggests the use of the theoretical cyber-RAT framework introduced in 2.6.3 as an aid to assist with theorising small-scale person-centric technological risk. Section 9.7 presents further evidence drawn from the findings to add to personal technology use as an augmentation of the traditional model of insider threat. Section 9.8 resolves **RQ3 IoT unexplored risk** with evidence of current IoT in the corporate space and a contemplation of emerging smart technology as a threat to the workplace of the future. The discussion concludes in 9.9 with brief reflection on the analytical process and signposting to the original contribution to be presented in Chapter Ten.

9.2 Limitations in the Research Instrument and the Survey Process

Errors observed in the survey logic were discussed in 7.2. These flaws affected the performance of the research instrument but did not impinge on the results. This next section describes lacunas observed in the raw data which subsequently affected the findings.

9.2.1 Respondent Error

It became apparent that participants had made occasional mistakes during the questionnaire and placed responses in the wrong field. This had triggered the skip logic and transported the respondent elsewhere in the survey, losing the opportunity to provide relevant data. On each occasion that a user's initial response provided data of value, but subsequent questions were left unanswered, a data-gap existed. In general, a scrutiny of later responses by the respondent would provide sufficient information to replace the missing data but occasionally the lacuna could not be resolved. Whenever the gap remained, the respondent had to be excluded from a particular data sample due to lack of conclusive evidence. An example of a data-gap affecting the overall results was observed in the IoT survey. Respondents who owned IoT units but not a wearable device were required to mark a box to confirm their circumstances. Skip logic would then facilitate the appropriate questioning. Thirteen respondents who stated that they owned IoT appliances marked the incorrect box and were carried out of the IoT survey without providing any usable data.

Data provided by other appliance owners provided some absent information, for example, confirmation that the accompanying command-and-control application

was downloaded to a personal device. It could be assumed that the thirteen owners would follow suit since it is understood that a benefit to the consumer is how IoT appliances may be operated via a smartphone (Smith, 2019). Despite this, it was not possible to speculate whether the thirteen users installed device updates, changed default passwords, brought the appliance to work or accessed it remotely from the workplace and they had to be excluded from those datasets. The literature identifies a growing trend for IoT appliances (discussed at length in 9.8) and results confirm ownership by several respondents. With no data to assist risk appraisal, findings are limited and can only signpost towards speculated risk, rather than confirming employee behaviours.

9.2.2 The Five-Point Scales

Average users in the sample were assumed to possess differing levels of ability and interest in technological systems and a five-point scale was used to ascertain likelihood or frequency of various digital activities. Participants were offered choices of ‘Always’, ‘Quite Often’, ‘Sometimes’, ‘Very Rarely’ and ‘Never’. Although results demonstrate that ‘Never’ is the highest occurring result, sufficient responses of ‘Always’, ‘Quite Often’, ‘Sometimes’ and ‘Very Rarely’ identified trends suitable for examination. Nonetheless, the frequency markers create limitations as they are too subjective to the individual, in particular the choice of ‘Very Rarely’. As explained in 8.2.2 and the recording of workplace digital activity, ‘Very Rarely’ may represent both an activity taking place very infrequently or one taking place often, but not as frequently as other activities. As a personal example, the researcher would say that she ‘Very Rarely’ uses Bluetooth, preferring to use communication apps to send files and media to other users. Nonetheless, when sharing files between personal devices, Bluetooth is used.

Hence, in this example, ‘Very Rarely’ entails an action which occurs at least once or twice every month, but not frequently enough to consider it as regular activity.

The indicators chosen for the five-point scales could not deliver precise data, but to use a meticulous marker would necessitate a respondent taking time for contemplation. Indicators were purposefully simple as the survey contained numerous queries and questions might be passed if the user was obliged to reflect at length on personal behaviour. Despite the ambiguity afforded to ‘Very Rarely’, it may be argued that those who irregularly conduct a particular activity should still be included in applicable datasets. The key finding is that activities most likely to cause harm take place in the corporate or personal space. In respect of the research questions, unsafe activity is relevant regardless how infrequently it may occur.

9.2.3 Passed and Unanswered Questions

It was observed that some respondents who had diligently provided answers would occasionally pass over a query. Some omissions were the final question in a series related to a particular topic, others were completely random. Examination of responses with unanswered questions could not determine whether the question was overlooked, or consciously evaded.

9.2.3.1 Accidental or Deliberate

The known failures in survey logic resulted in *all* participants passing the same enquiry or sequence of questions. This suggests that a single question was unlikely to have been accidently missed if answered by all other participants. It can only be assumed that “question threat” (Foddy, 2011, p. 117) occurred and

disconcerting questions were deliberately avoided. To place this in perspective, seventy-two participants confirmed a profile on LinkedIn, but twenty-five passed the next question in the sequence which queried the type of personal information made available on their profile. The options for respondents to select were typical to that found on most LinkedIn profiles and included educational establishments, voluntary work, sports and leisure activities. The question had topical relevance since information of this type was effective as an open-source resource during 'Executive Risk' (Chapter Five) and is of value to attackers for social engineering (see 5.4). The twenty-five respondents may have passed the question because they included no data of that type on their profile page and the enquiry had no relevance. Alternatively, when reading through the question it may have been apparent how personal data can be amalgamated to provide an instant profile to any unsolicited viewer. The question may then have been avoided to prevent any further self-examination or possible recriminations.

In addition to avoiding uncomfortable or supposedly irrelevant questions, some queries may have been dismissed if the participant was short of time. A respondent may have wished to complete and submit the survey but could not afford time for rumination. Thus, any question that could not be answered instantly was passed over. It is assumed that a bored respondent would have abandoned the survey and no further data would be collected but in all instances of passed questions, the questionnaire was completed and submitted. Thus, it can only be assumed that a skipped query was a personal and deliberate choice.

9.2.3.2 Anonymity

It was noticed that some respondents deliberately passed any questions which threatened their anonymity. For example, RN58 stated gender, age, nationality and education but left the occupation field empty. RN58 is from Hungary and declaring her job status may enable identification if she is the only Hungarian national in that role in the organisation. This suggests that despite the actual anonymity made possible by the survey software, some participants preferred to take extra measures to ensure that identification was not possible.

9.3 The Findings

It should be clarified that not all respondents demonstrated poor cyber safety and lack of awareness. The majority of those who connect their personal device to the corporate network answered 'Never' when asked if potentially 'unsafe' digital activities took place at work. Twenty-eight percent use antivirus software and fifty-seven percent install updates when prompted. Nonetheless, 'unsafe' behaviours including downloading apps and the use of applications to access specific web-based services were adequately demonstrated by the sample. The following discussion will therefore focus on respondents who satisfy the requirements of the research questions and 9.3 will elaborate on findings relevant to some of the observed 'unsafe' behaviours.

9.3.1 Apps

Apps are one of the primary attributes of a mobile device and fundamental to contemporary technology. Unsurprisingly, most of the sample (eighty-six percent) confirmed regular downloading of applications to personal devices. Table 20

(below) acts as an aide memoire for the remainder of section 9.3 and recapitulates the app-based activities described throughout this work as potentially ‘unsafe’, alongside the percentage of the overall sample (N=76) who actively participate in each one.

Applications	Percentage of Respondents
Communication	96%
Social Media	86%
Gaming	33%
Streaming	28%
Adult	14%
Dating	12%
Casinos	4%

Table 20. Apps for 'Unsafe' Activity

The evaluation of routine digital activity using mobile apps (7.4) elaborated on the known security risks which may affect applications and the potential for threat generated by specific categories of apps. Findings confirm that devices brought into the workplace are used for these plausibly unsafe behaviours, that some activities take place at work, and some occur whilst devices are connected to the network. Apps for social media, video streaming, gaming and communication are presumed to be responsible for introducing malware into an organisation (Ashford, 2019b). Use of apps thus satisfies requirements of **RQ1 actual/perceived risks** and actual risk and provides understanding of device use in accordance with potential impact as investigated by **RQ2 average usage/impact**.

9.3.2 Communications Apps

The findings confirm the literature which proposes that instant messaging is becoming the preferred method of communication in the financial sector and replacing email between remote colleagues (Dungay, 2019). Communication apps are the most popular activity undertaken with a personal device (see Table 18, 9.3.1) and ninety-six percent use them in personal space (see Figure 32, 8.6.1). Ninety-six percent of the sample use WhatsApp and Facebook Messenger in the workplace (see Figure 35, 8.6.4) although the data does not confirm whether this an organisational requirement or an employee's personal choice. The literature identifies that WhatsApp and Facebook Messenger have been known to share malware (CisoMag, 2020; Lutrum, 2019; Palmer, 2017a; Palmer, 2018) and are alleged to be amongst the most unsafe applications found in the workplace (Appthority, 2018). Using cyber-RAT to evaluate communication technologies identifies that instant messaging may act as an instrument-in-technique and the user or organisation (or both) may take position of suitable target. Hence, in respect to **RQ1 actual/perceived risks** and **RQ2 average usage/impact**, an actual risk of employees inadvertently sharing harms between devices and/or threatening the network is present and use of devices for web-based communication may be an unmitigated threat.

WhatsApp has two billion subscribers and is the most popular instant messaging service (Singh, 2020), confirmed in the results by one hundred percent of the communication app sample stating that WhatsApp is installed to devices (see Figure 34, 8.6.3). WhatsApp promises strong encryption to protect data from "hackers and criminals" (WhatsApp, 2020, para. 5) and average users may

assume that the encrypted app is a capable guardian, not comprehending actual capacity for harm enabled by instant messaging. Nonetheless, cyber-RAT recognises that the potential for receiving malware places the user as suitable target. Fluidity enabled by cyberspace may then position a WhatsApp user and a compromised device as a tool to extend the reach of an attacker. Without awareness that instant messaging can be misused as an attack vector, an average-user employee cannot make an informed choice about using it in the workplace. This thus highlights a major finding, first speculated in Chapter Two (2.5) and then confirmed throughout the analysis. Financial sector employees would benefit from specifically tailored cyber-awareness to empower an average user to recognise where personal choices may create risk to self or others. An organisation investing in training bespoke to digital activities of each individual employee may thus enable 'guardianship in action' (Reynald, 2009) where a guardian available and capable of intervention is present (see 2.5.2). This discussion is elaborated further in 9.5 of this chapter and the use of cyber-RAT as an aide to risk management is proposed in 9.6.2.

9.3.3 Absent Data

Despite theorising that communication apps may be an unmitigated threat; the results are limited as no data of value was captured other than that recorded in 8.6. Seventy-nine percent of employees use two or more communication apps (see Figure 33, 8.6.2) and Figure 34 in 8.6.3 illustrated the popularity of WhatsApp, Facebook Messenger and Snapchat amongst respondents. Results would benefit from thorough exploration of workplace use of communication applications, for example, type of content sent between users and whether

colleagues use instant messaging to communicate inside the office and outside the corporate environment. More importantly, whether corporate files are sent or received, particularly as friendships formed between colleagues may result in critical data shared in and out of the workspace.

The lack of additional data prevents theorising whether employee use of WhatsApp or Messenger should result in restricted or controlled access during enterprise time, or whether corporations should supply (and insist upon) antivirus solutions to enable guardianship. The literature suggests that managers have failed to incite staff to engage with secure systems offered by the enterprise as a method for employee communication (MacDonald, 2019). Lack of uptake may be because internal (business) resources, although protected by security, might be monitored by managers. External methods such as WhatsApp and Facebook messenger offer privacy and since users are familiar with text input on their own devices, may be a faster communication option. In addition, familiar apps offer emojis and facility to attach files and media. Data confirming whether employees limit use of communication apps to personal activity or whether they have become utility tools inside the workplace would have enhanced the response to the research questions. Without additional data it can only be concluded that communications apps have potential to impact upon the network and should be addressed by risk or security managers.

9.3.4 Streaming and Piracy

Copyright protected content accessed by streaming and (or) gaming has relevance to both **RQ1 actual/perceived risks** and **RQ2 average usage/impact**

but not in respect of employees conducting illicit activity. The evaluation of apps in 7.4 described how popular media and games are exploited as methods of attack. Distributors of illegal pirated content accept payment for placing malware where it will be encountered by users (EUIPO, 2018) and employees viewing content intended for a subscription service may expose devices to threats. For example, a streaming website offering free content may have been infected with compromised code (EUIPO, 2018) or malware can be included with a downloaded file (Paganini, 2019). In the context of cyber-RAT, users accessing 'free' content place themselves as suitable target and a compromised device may become an attacker-in-technique.

It is probable that conventional risk assessments do not consider devices used to watch film or television as a potential threat, but contemporary piracy is a growing concern. Subscription providers offer unlimited access to content but despite this, an estimated eight million British viewers (8000,000) view copyright protected material (Snelling, 2019). Piracy is expected to increase in response to viewer demand (Thibeault, 2018, p. 10) and the trend may be exacerbated as some legal streaming methods can be modified with applications to obtain content which should be paid for (Pratt, 2019). Subsequently, users may view copyright protected material without intending to commit an illicit activity, merely assuming that what they watch is free. As an example, the researcher personally knows average users who regularly stream copyright protected content and do not recognise it as an offence. They simply wish to access material unobtainable on their subscribed services and use free facilities available on the internet to accomplish the task.

The research instrument asked if personal devices were used to “stream recently released films and new media” and to “view films or videos streamed from file-sharing sites or cyber lockers”. The questions were specifically phrased to ascertain whether copyright protected material may be accessed, without asking a direct question. The phrase “recently released films” was used to imply motion pictures still on theatrical release as these may only be viewed by accessing pirated content. File-sharing sites and ‘cyber lockers’ are two popular ways to access illicit materials thus it was anticipated that respondents familiar with the terms would know they were being asked about copyright protected content. The results confirmed that twenty-one percent stream new media and films and twenty-two percent would ‘Always’, ‘Quite Often’, ‘Sometimes’ or ‘Very Rarely’ view media from file sharing sites or cyber lockers.

The data satisfied the objectives of **RQ1 actual/perceived risks** and **RQ2 average usage/impact** by confirming that streaming takes place on devices both in and out of the workplace. Nonetheless, asking the questions using nondescript terminology could not confirm an *actual* risk of malware infection by access to copyright protected content. It cannot be ascertained whether the respondent answered affirmatively because they subscribe to a streaming service, watch videos on YouTube and think this is file sharing, or are regular users of websites where pirated material is available to access. Malware developers are capitalising on users’ preference for streaming and are producing malicious apps specifically to access free content (Batt, 2019) and the literature suggests that “millions of smart devices have been infected in global scale” (Nikas, Alepis and Patsakis,

2018, p. 81). Data confirming *actual* streaming activity conducted by financial employees would have had real value.

To achieve conclusive data, it would have been necessary to ask respondents if they engage in activity recognised as illicit. Regardless of whether a respondent considers their streaming activity to be dishonest, a University Research Ethics Committee may consider asking the question to be a breach of the principle of malfeasance (University of Derby, 2011). The researcher's apprehension about violating ethical standards resulted in the nondescript phrasing described above which may have been misunderstood and failed to collect significant data. On reflection, a solution may have been to ask respondents whether they would "consider" free access to media content or 'cracked' or 'patched' games (7.4.4), thus avoiding question threat and causing harm. Respondents would have retained the option to avoid the question, but those who routinely access free content may have provided data. An improved appraisal of risk might then have been achieved. The researcher had been advised to avoid questions relating to the use of 'adult sites' as they would not be answered but respondents did provide data, thus confirming that anonymity enables people to talk about topics considered to be 'sensitive'.

9.3.5 Absent Data Affecting the Value of the Findings

Throughout the analysis, several lacunas where key data is absent became apparent, and significant themes identified in the results are not adequately addressed due to limited available information. The findings have theorised areas of concern applicable to the research questions, but specific behaviours cannot be definitively confirmed, and only speculative conclusions can be reached about real

and present risk. The first part of this chapter (9.2.1) discussed how respondent error during the survey had resulted in key IoT data missing from the results. In 9.3.3, the lack of data evidencing workplace uses of communications apps came from insufficient questioning. Data was not captured as extending a line of enquiry would have added to the already lengthy survey, thus, data collection was limited by space.

Other lacunas were created by fear of breaching the boundary of non-malfeasance required by university research ethics (University of Derby, 2011). This caused questions to be omitted or entailed use of weak terminology resulting in data with no clarification that the question was understood as intended. Section 9.3.4 detailed how fear of causing harm *prevented* seeking data to confirm risk of threat from pirated content and an example of a topic *omitted* through fear of malfeasance is 'jailbroken' or 'rooted' smartphones. The enquiry regarding 'hacking' the operating system to modify a smartphone to personal taste (see 3.7.2) was removed from the research instrument due to apprehension of surveying potentially dubious activity. Although the practice is not presently illegal, adapting a device removes safety features, leaving it vulnerable (Johansen, 2020) and sometimes unable to install updates or security patches (Snyder, 2019). Routine internet use might then introduce harm and security experts recommend that IT managers should monitor presence of modified devices in the workplace (Snyder, 2019). Questions about activity that could threaten organisational security may have caused unease for respondents, hence the decision was taken to omit the enquiry. This was further justified by

assumption that device modification may be too niche a topic to be relevant to all average-users.

Although not recorded in the results, the respondents were asked to rate their technical ability. Many claimed expert level technical skills in coding and software development, therefore, modification of smartphones to suit personal taste may be an actuality. Popular software enabling access to streaming and additional content does not function on an iPhone unless it has been jailbroken (Woollaston, 2018) and a desire to access free content may encourage iPhone users to tamper with the iOS to install unauthorised apps. An android user with a malicious streaming application installed may enable an attacker to "penetrate more networks than he initially could" (Nikas, Alepis and Patsakis, 2018, p. 82) and thus an infected device may not only affect the corporate network, but any Wi-Fi connection made in transit. Jailbroken devices have been identified as a contemporary threat to organisations (Symantec, 2019, p. 41) and choosing to omit the question from the investigation lost an opportunity to ascertain whether employees engage in the practice. Failure to confirm whether modified devices are a real and present risk in the financial workplace is a limitation in the results.

9.3.6 Security Risks of Applications: Outdated Software

The risk of continued use of outdated applications was discussed in context of users not removing old and unused applications from personal devices (see 7.6.2). A contemporary development is that outdated mobile operating systems will no longer receive support (BBC News, 2020a). Manufacturers regularly issue upgraded models offering innovative new features, but the user is not obliged to

purchase the new system. A favoured unit with a familiar operating system and no apparent faults can be used for the remainder of the device lifecycle if the user chooses. If the manufacturer withdraws support without user awareness, an operating system no longer receiving security updates may remain in use indefinitely. Any identified but unpatched software flaws will render the device vulnerable to malware or other harms encountered during routine internet activity.

9.3.7 Security Risks of Applications: Updates

Installing recommended updates for applications or the operating system is a necessary security measure to maintain safety and ensure optimal software performance. In the context of the cyber-RAT framework, regular updates enable capable guardianship and without them a vulnerable device places the user as suitable target. Guardianship is then reliant on user-cognisant cyber behaviour and enabled guardianship in the form of antivirus solutions. Figure 19 (7.6.1) illustrated that thirty-eight percent of users accessing the network did not accept regular security updates. The action of connecting an unsecured device to the network suggests that the user-as-guardian is absent, and cyber-RAT places the organisation as target. Guardianship is subsequently forced to rely on technological solutions. A sophisticated attack using polymorphic malware capable of circumventing traditional detection methods (see 3.3.2) may successfully compromise the network. In respect to **RQ1 actual/perceived risks**, an employee accessing the internet with inconsistent device security may be an unmitigated risk and in regard to **RQ2 average usage/impact**, devices without regular updates cannot be considered as secure. A solution to improve corporate security may be to raise awareness of suitable targets enabled by ‘unsafe’

behaviour and equip the user with guardianship capability. This concept is discussed further in 9.6.2.

A user may choose to temporarily delay an installation to prevent impaired performance or functionality of a device while the download is taking place. An update may additionally be avoided to prevent a permanent modification to a favourite system or app. Avoidance of this type is verified by an internet user who posted a comment to a security forum to declare her refusal of an update. If necessary, she would 'root' (make modifications to) her phone to prevent changes to the operating system (Ryan, 2015). Users with advanced technical skills may routinely take action to prevent apps or systems from updating and changing aspects of their performance. Many respondents reported advanced and expert level ability and the modern financial sector is likely to have thousands of highly competent employees. Evidential data to confirm any connection between technical competency and rejected updates may have augmented the response to the research questions.

The results related to updates are another example where real and present risk cannot be adequately confirmed. The question was structured to collect data about apps and operating systems but on reflection placing systems in separate categories may have elicited a more valid response. To explain with perspective, the findings may be limited as users who will update an operating system but not their installed apps may still have responded affirmatively, and vice-versa. Conducting examination as individual categories would have aided a more concise evaluation of user behaviour.

Current UK statistics indicate that UK financial services employ approximately one point one million workers (1.1000,000) (Cherowbrier, 2020). Since results reveal that seventy-six individuals bring a total of one hundred and nine (109) devices to their workplaces, it may be assumed that a significant number of apps and operating systems are present in financial enterprises. Extrapolating the number of respondents who connect devices to the network and the percentage of that group who do not regularly update (see Table 11, 8.4.2), suggests that approximately one hundred and eighty-eight thousand (188000) unsecured devices may be accessing financial networks.

The following contemporary example may assist to illustrate the dangers of avoiding software updates. Microsoft has been encouraging users of the Windows operating system to update from the outdated Windows 7 to Windows 10. Consumers who favour the older version are unwilling to accept the modifications that the update will entail and continue to refuse the update (Allan, 2019; Allen, 2020). In early 2020, Microsoft withdrew support for Windows 7 and no further patches will be issued to repair flaws and errors in the code. As a result, “malware targeting Windows 7 increased by 125%” (Webroot, 2020, p. 7) when criminals recognised a soft target and took advantage of user preference for a familiar system. Security researchers have observed that twenty-five percent of business PCs continue to run the now unsupported Windows 7 (ibid., 2020, p. 7). Figure 22, in 8.2.1 illustrated that the desktop computer is the most common company issued device used by employees for personal digital activities including downloading apps, social media and games (see Figure 23, 8.2.2). The actual risk identified by **RQ1 actual/perceived risks** that employees are using company

issued devices for digital activities may be exacerbated further if the PC is using an unsupported operating system. A further example to illustrate a possible outcome when a security update is not installed is the 2017 ransomware attack which affected two hundred thousand global users from one hundred and fifty countries (BBC News, 2017). This exploit is documented in Appendix I.

9.4 Social Media

According to the literature, social media use may introduce harm by two distinct methods. Inadvertent access of malware or other threats shared through interconnected networks (Sood and Enbody, 2011; Symantec, 2016) and exploitation of personal content available on profile pages belonging to the user and their network (Jagati et al; 2007; Tsikerdekis and Zeadally, 2014). Targeted attacks are the contemporary method for criminals to assault a corporation (Symantec, 2019; Webroot, 2020) and findings documented in 8.5 imply that employees may be suitable targets for a focused assault. This is endorsed by the practical research recorded in 'Executive Risk' (Chapter Five) which established that personal data available online about executive level employees might be exploited by an attacker.

In respect of inadvertent access to internet threats, social media habits illustrated in Table 14 (8.5.3) suggest that actions known to place users at risk of convergence, including following links to view sensationalist content or to win prizes (BBC News, 2016; Christenson, 2003; Dharmavaron, 2015) take place with varying regularity. Eighty-six percent of respondents use personal devices for social media and sixty-one percent maintain profiles on at least two social media

sites. The literature suggests that a social networking employee will regularly check their profiles (Harari, 2017; Stubbington, 2017) and each time social media is accessed the user may become a suitable target. When behaviours known to exacerbate risk occur regularly, a device may be at risk of social media harms throughout the day. If connected to the corporate network when convergence occurs, cyber-RAT suggests that a device may become an instrument to extend reach of an attacker and an employee sharing content with colleagues becomes an unwitting assistant to the assailant. In light of the results demonstrating employee use of social media (8.5), the capacity to threaten a network is relevant to both **RQ1 actual/perceived risks** and **RQ2 average usage/impact**.

9.4.1 Oblivious Social Networking

All users are at risk of encountering threats if navigating social networks with no care or attention given to what content is viewed. Inattentive browsing might include spontaneously following links to appealing content, accessing media files from unknown sources or responding to unsolicited comments. Opportunity for nonchalance-induced harm may be exacerbated if a user believes their device is protected, either by corporate firewalls, user-enabled guardianship such as antivirus and updates, or by 'inbuilt' security. To place this in context the data showed that one hundred percent of the iOS users who connect devices to the network use social media in personal space and seventy percent admit using social media at work with varying frequency. The comments seen in Table 8 (7.6.3) implied that iOS users have unerring 'faith' in the security of an Apple device and social network activity may reflect this sense of guardianship. Any appealing content may be accessed regardless of origin or apparent legitimacy,

thus resulting in a greater risk of convergence. The concept of enabled guardianship as a contributor to theorised risk is discussed further in 9.7.3.

9.4.2 Work Colleagues as Social Media Friends

Eighty percent of respondents indicated that they would 'Always', 'Quite Often', or 'Sometimes' accept work colleagues into their network of acquaintances. This is recognised in the literature as a 'blurring' of personal and organisational social circles' (Wilcox and Bhattacharya, 2020, para 1). There is no intrinsic reason why individuals should not become social media friends with work colleagues, but the issue of privacy may be pertinent. A conscientious user determined to protect a profile must ensure that other members of their network are proactive with privacy enhancing technologies such as privacy controls. Digital footprints left between social media friends may be exploited, unless the user-network is dedicated to restricting access by unauthorised viewers. Accordingly, unprotected social media profiles are significant to **RQ1 actual/perceived risks** and potential for harm instigated by employees. It may be possible to convince family members of the necessity to comply with a request for privacy controls, but work colleagues may not be so amenable. Having accepted a colleague as a friend, it might not be possible to 'unfriend' them without causing offence and creating an 'atmosphere' amongst staff in an office environment.

A second relevant issue is that of relationships. A prospective attacker gathering intelligence may observe that a director of a small company could be used as a 'gateway' to a larger corporation due to relationships observed on social networks. Social engineering might be used to befriend an individual because of opportunity

to access a key member of staff visible on their list of friends. The practical research in Chapter Six, 'A New Direction' observed that many directors of small or medium enterprises launched an independent business after a career spent working in large international corporations. Individuals who were colleagues in other organisations may retain a professional or friendly relationship and personal networks might contain high-ranking individuals of interest to an attacker. Security research has observed phishing attacks where emails between colleagues have been exploited by an attacker who attaches a malicious file to an ongoing correspondence and forwards it to the victims' network. As the conversation details are real, the email appears credible to the recipient and the corrupt file is accessed (Webroot, 2020, p.16).

An employee with work colleagues in their social network might be used to gain access to a member of staff with superior value as suitable target. In respect to **RQ1 actual/perceived risks**, social media relationships may be exploited in social engineering attacks. This again highlights the importance for all acquaintances in a social group to maintain active privacy and bespoke training may assist to raise awareness of the risks of social media use. As an additional measure it may be necessary to enact policies expecting compliance towards privacy if employees are likely to become friends on social media.

9.4.3 User-Content about Children as an Aid to Attackers

Respondents who confirmed posting photographs and making comments about their children on social media pages came from the thirty-five to forty-four and forty-five to fifty-five age demographics. These results are consistent with the

practical research where it was observed that users aged thirty-five to forty-four with young families were most likely to share information regarding children and family life. The marginally older forty-five to fifty-five demographic were seen to be sharing images of grandchildren or embarking on new parenthood after a second (or third) marriage. From the perspective of an assailant, images and comments about children typically invite responses from friends and family in a personal network. These responses may then enable identification of crucial relationships, establish significant names and events and assist with compiling sufficient data to support credibility. To illustrate with perspective, the social engineering framework (Mouton, Leenan and Venter, 2016) guiding the practical research in Chapter Five, 'Executive Risk' confirmed the literature by selecting a 'target' for the position held in the company and supposed value to an attacker (Burns, Johnson and Caputo, 2019). The digital investigation observed parents and grandparents sharing news and special events with extended family. The casual approach to profile privacy made personal data about executive level staff from a multi-national corporation available to the tenacious theoretical 'attacker'. In the context of cyber-RAT, content about children on social media places a user as suitable target. Since any parent is likely to respond to a phishing email referencing accurate details about a son or daughter, the organisation may also be at risk of convergence.

9.4.4 Heritage Content

The methodology chapters demonstrated how data available on LinkedIn can be used to corroborate fragments of personal information gleaned from accessible profiles on Facebook, Instagram and Twitter. For example, a profile photograph on LinkedIn may contain the same background as other pictures on Facebook.

Mention of voluntary work or leisure pursuits in a LinkedIn profile may be confirmed by posts and photographs on other social sites and the combination of sources can easily provide sufficient data for an attacker to prove credibility. Social media users may benefit from demonstration that privacy enabled on a personal profile is not always sufficient. A determined social engineer can obtain data about a user with a private account by searching for others suspected to be in a network to find one without the same level of privacy.

The nature of social media entails that dynamic searching can often retrieve archaic material, particularly if it has been shared or modified by other users. Even content deleted from a user's own pages may still be available to find via other profiles. Using respondent data to illustrate, Table 17 in 8.5.6 illustrated the frequency that social media users post content known to be of value to social engineers. The highest percentages shown in Table 17 represent those who claimed that they 'Very Rarely' post content of this type. Nonetheless, section 5.4 in 'Executive Risk' (5.4) established that legacy content can be retrieved from anywhere in a user's social network. Even content posted 'Very Rarely' may be of value if obtained by a tenacious attacker.

To safeguard personal data, a user should take ownership of privacy and ensure that their network is proactive about preventing unsolicited viewing by others outside their social group. If social media is assessed using cyber-RAT, increasing guardianship from various sources may reduce the chance of convergence created by routine activity. Capable guardians may include the user's employer who raises awareness, the network of acquaintances with

sufficient controls in place to prevent misuse of exploitable data and the user-guardian conducting constant due diligence.

9.4.5 The 'Narcissistic' Social Media User

Chapter Four 'The Corporate World' identified narcissistic tendencies (Bergman et al, 2011; Carpenter, 2012; Wang, 2017) in social media users (see 4.10) and suggested significance to **RQ1 actual/perceived risks** and **RQ2 average usage/impact** on account of personal data accessible in unprotected content and self-portraits (selfies) most likely produced by a personal device (4.8.5). Evidence of the narcissistic user was seen again in Chapter Five 'Executive Risk' (5.4.3) where profiles of attractive users contained 'selfies' intended to incite responses from other users (Wang, 2017) and flattering comments left by other users customarily revealed crucial data. The predictable behaviour of attractive users became a resource for usable data to confirm identity, enable keyword searches and locate accounts belonging to family and key relationships (see 5.4.3).

In accordance with the traits suggested by the literature (Bergman et al, 2011; Carpenter, 2012; Wang, 2017) fifty-three percent of respondents routinely publish 'selfies' to social media profiles (see Table 17, 8.5.6). A narcissistic user might post their images to many profile pages and knowingly forgo privacy enhancing technologies so that others outside their network may offer positive feedback, thus generating vast quantities of data lacking guardianship. In regard to **RQ1 actual/perceived risks**, a prospective attacker following the social engineering framework (Mouton, Leenan and Venter, 2016) may also acknowledge behavioural traits in users who regularly publish self -promoting content and recognise that social media narcissism may equate to suitable target. The

respondents confirmed in Table 17 (8.5.6) that ‘selfies’ are posted using personal devises, thus indicating that routine activity for a narcissistic user may be regular publishing of self-promoting content and visiting profiles to review responses. In respect to **RQ2 average usage/impact**, a device used for frequent access to social media is at risk of convergence with malware or other harms and thirty-two percent of respondents confirmed maintenance of at least three social media profiles (Figure 30, 8.5.2). More than one hundred and eighty-six (186) social networks exist on the internet (Wikipedia, 2019) and the average user is assumed to have up to eight active profiles (Kemp, 2020). Thus, results relating to respondent profiles may be limited as the research instrument did not query use of newer or niche networks. A narcissistic user may be frequently accessing multiple social media applications in search of the ‘dopamine hit’ (Parker, quoted in Lanier, 2018) allegedly felt whenever content receives a positive response. This further highlights necessity for bespoke awareness in alignment with personal activity. A narcissistic user may not wish their profiles to have active guardianship but might be guided towards recognising need for control when other users or a corporate employer may be threatened. Risk of convergence by excessive access to social networks might be mitigated by enabling basic device guardianship once a narcissistic user has appreciated social media as an attack vector and equated personal use to suitable target.

9.5 Recommendations to Enhance Bespoke Training

The objective of the central investigation is for financial corporations to acknowledge the human element when assessing risk and accept that cybercrime is not always a technological issue. Despite evidence in the data that some

respondents enable guardianship in the form of antivirus and regular updates, basic device security may not be sufficient to defend against sophisticated internet threats. Human guardianship would be significantly enhanced by education and awareness, therefore 9.5 will recommend issues drawn the results that might be addressed during bespoke training. A “fear appeal” (Johnston, Warkentin and Siponen, 2015, p. 114) in the form of generic awareness and training will typically focus on risk to a users’ “information assets”. Despite a real and present threat, the impact is not “universally personally relevant” as average-user acceptance of the relevance of assets is “highly subjective, thus potentially marginalizing(sic) the impact” (ibid, 2015, p. 114). Without experience of loss, users will not comprehend digital risk in the same way as those who understand harm (Rughiniş and Rughiniş, 2014, p. 113).

If the literature is correct and only those with experience of victimisation will acknowledge personal internet threat, security managers must avoid alienating employees who think that cyber security has no relevance to their circumstances. This may be achieved by acquiring knowledge of employee personal technologies, equating contemporary risk with individual digital activity and empowering the user with knowledge directly applicable to their circumstance and lifestyle. Risk and security managers may not be constricted by the ethical restraints placed upon academia and if able to guarantee anonymity to employees, may find that members of the networked community are happy to discuss their activities in cyberspace. The concise and direct questioning unavailable to an academic researcher might therefore obtain data of value. Although the results recorded in this thesis cannot provide conclusive evidence of

risk, the findings confirm that unsafe activities take place on devices connected to the corporate network and are of value to personalised training.

9.5.1 Applications Intelligence

Employee use of applications in and out of the workplace may constitute a significant unmitigated threat to the network. Any organisation employing a policy of BYOD or allowing personal devices into corporate space may be certain that a considerable number of applications will be present. Technology journalists publish key findings whenever security researchers produce quarterly threat reports and typically identify any malicious apps in circulation (see Doffman, 2019; Palmer, 2020b; Scroxton, 2020). Hence, knowledge of users' preference in applications might be used in conjunction with security literature as an aide to bespoke training. If specific popular applications are announced as harmful by the security industry, then managers may share knowledge with applicable users who can apply guardianship, for example antivirus, app deletion, or the device left outside the workplace.

Since app popularity and user trends regularly fluctuate, knowledge of employee preference for service provision may have greater impact. As an example, entertainment apps have been identified as particular targets for attackers (Symantec, 2019) and results show that many users routinely use devices for entertainment in both personal space and the workplace (see 8.3). Security issues are the possibility of downloading malicious code masquerading as legitimate software, and the risk of accessing malware whilst using apps to access specific entertainment content. An understanding of categories of service will

enable training to focus on personal activity rather than specific app use. In the example above, an employee using apps for streaming or playing games might be guided to inspect entertainment applications for legitimacy and ensure that antivirus and malware solutions are installed. Instead of recriminations about any access of copyright protected material, users could be informed about harms and taught to recognise specific locations notorious for advertising or providing pirated and infected content. Bespoke awareness will empower the user to make informed choices about personal behaviours (Rughiniş and Rughiniş, 2014) and may prevent harms from entering the workplace.

Bespoke training may provide additional benefit as a two-way knowledge exchange between users of corporate systems and those employed to protect them. A user's routine digital activity may remain consistent, but cyber criminals regularly update their attack methods. The contemporary multi-tasking assailant may combine multiple methods into a single assault and include phishing emails, trojan malware, and malicious code to exploit vulnerabilities in software or applications (Webroot, 2019, p. 20). So that training may remain effective, risk and security managers will require up-to-date knowledge of contemporary threats alongside an understanding of behaviour which may facilitate introduction of harm. Regular appraisals of employee digital activity will empower security managers to recognise user-trends, emerging technologies and developments in 'unsafe' behaviours which might require enhanced enterprise technical solutions.

9.5.2 Enhanced Security

Bespoke training may assist some users to recognise the benefit of regular updates and additional security in the form of antivirus solutions, but it is unlikely that all users will be persuaded. Those who will not accept manufacturer modifications to apps or operating systems and those who refuse to pay for robust technological services will probably remain unconvinced. Bespoke training will therefore assist security managers to establish where lacunas in device safety may threaten overall security. If employees cannot be convinced to improve personal security, then it may benefit the organisation to ensure that technological solutions are sufficiently vigorous to withstand absent user-guardianship. Options may be to provide a correctly configured guest network (see 8.8.5 and Appendix G) and allow employees to continue with personal digital activity. Staff will receive internet access and corporate files necessary for work purposes whilst critical data is stored on a separate network only accessible via a company device. Alternatively, the organisation might consider investment in robust antivirus /anti-malware solutions for all devices on company premises and invite employees to install it to home systems as an extra measure to prevent sharing harms. If continual appraisal suggests non-compliance to recommendations for regular updates and use of antivirus, organisations may have to curtail BYOD and personal technologies on premises and supply company issued devices pre-loaded with robust solutions. Personal digital activity may continue but any absent user-guardianship would be mitigated by up-to-date software.

9.5.3 iOS Users as a Challenge to Security

The findings in 7.6.3, supported by users' comments in Table 8 revealed that iOS users have an apparent faith in the infallibility of their Apple device. This may detrimentally effect enterprise security if an employee's belief in enabled guardianship influences digital activity and attitude towards cyber-safety. Since users of personal technologies are likely to be familiar with *some* internet threats, iOS users may have invested in an operating system ostensibly secure against malware and other perceived harms. The iOS has (alleged) guardianship capabilities and supposedly offers protection during regular interaction with the internet, applications and web-based communication methods. Using this model, Apple owners may see themselves as conscientious users, protecting self and devices. An alternate theory suggests that Apple devices are luxury goods (Kemper, 2018a), renowned for stylish and innovative products (Viswanathan, 2019) and consequently an iPhone may be a lifestyle choice. It is therefore a fortuitous circumstance that Apple take a robust stand against harms and the individual need take no further responsibility towards device security. The safety aspect of a luxury product may not have been a priority when choosing a device, but this model suggests that a capable guardian has been enabled, despite no intent or action from the user, other than the desire to purchase an iOS device.

Despite the assumed safety of iOS, the assumption of infallibility may be flawed. Security research asserts that the Apple operating system may be susceptible to internet threats and attacks have succeeded (Golubev, 2019; Goodin, 2019; Hay Newman, 2019; Kokh, 2019; Seals, 2020; Whittacker, 2019). The models described above may instead indicate an *absence* of capable guardianship. If

iOS is not unassailable, then unrestricted digital activity may allow convergence of offender and target. To place this in context, iPhone users surveyed during this project stated routine internet activities included visiting adult sites and online casinos. The activity per se is not at question, the concern is that some online services are renowned for spreading malware. A user with presumed security may have no inhibitions regarding content accessed or sites visited, but the guardianship assumed to be preventing convergence with an offender or instrument may not be present. Rughiniş and Rughiniş (2014, p. 113) concluded that those who have not experienced loss will not appreciate technological harm and comments illustrated in Table 8 (7.6.3) appear to confirm the literature. As an example, when asked why no antivirus solutions were used, RN35 asserted “I have never had any issue with security and keep my iPhone software up to date”. Although RN35 does install updates, the reason given for no additional security measures was the lack of personal or associated experience with digital harm.

It may be argued that owners have a responsibility to maintain secure devices, and this can be achieved by enabling basic solutions in the form of antivirus software and regular maintenance of apps and operating systems. Accordingly, the over-reliance on in-built security observed in iOS users may need to be addressed with iOS specific training and guidance towards extra protection of devices. Apple only permits approved apps and does not make any antivirus applications available for users to purchase (Yablokov, 2018). Nonetheless, iOS users who suggest that no antivirus is available (see Table 8, 7.6.3) are not entirely correct. Security researchers who acknowledge the existence of iOS targeting malware, recommend that Apple users are cyber aware (Yablokov,

2018) and advise installation of iOS specific security solutions (Williams and May, 2020). Examples are tools to check for weak settings and unsecure connections (Yablokov, 2018) and website blockers to prevent the iPhone from reaching a malicious site (Williams and May, 2020). It may be assumed that being cyber aware includes some understanding that threats may affect an internet user, therefore cyber aware iOS users checking settings and connections would acknowledge the potential for their device to be attacked. The comments seen in Table 8 (7.6.3) suggest a profound belief that iOS is a secure system unable to be affected by external harms. This thus implies that the iOS sample may not be cyber aware in respect to current threat alerts.

A “fear appeal” intended to “manipulate” users into acknowledging risks and applying protective remedies (Johnston, Warkentin and Siponen, 2015, p. 114) is unlikely to influence those who consider themselves protected. The challenge for risk or security managers is to enlighten users with no personal experience of loss and a fixed belief that guardianship is present and needs no reinforcement. The solution may be person-centric education to broaden the user perspective. Modification of behaviour may then follow as a consequence of equating personal activity with actual risk. Comments in Table 8 (7.6.3) suggest that iOS users have no knowledge of availability of security options for their operating system, thus the organisation could assume guardianship and take responsibility for supplying solutions. As an example, a robust suite of security solutions specifically designed for iOS (Williams and May, 2020) as an application available for download to multiple devices. Enterprise guardianship might then continue in the

form of app maintenance, regular appraisal to assure compliance and routine bespoke training to maintain user-guardian capability.

In addition to iOS users, remarks were left by users of other operating systems to justify rationale for not using antivirus. Comments presented in Table 9 (7.6.4) established lack of awareness, lack of interest and concern about cost as reasons for lack of security. The literature suggests that antivirus may be ignored since it may impair processing speed (Zhang, Raghunathan and Jha, 2014), but no respondent remarked that maintaining performance was incentive to forgo security solutions. If processing power is not relevant, employees may be willing to adopt antivirus if the enterprise-as-guardian supports the cost of robust solutions. User-level guardianship would be enhanced as default and a reduced risk of victimisation for the user may subsequently improve overall enterprise security.

9.6 The Cyber-RAT Framework in Action

The previous section suggested issues arising from the findings which if addressed during bespoke training may assist with enhanced organisational security. The following discussion proposes cyber-RAT as a complement to bespoke training, to assist managers and employees to recognise where activity may position users or other entities as suitable target; and suggest opportunities for enabled guardianship.

9.6.1 Routine Digital Activity

Each activity illustrated in Table 20 (9.3.1) was included in the research instrument due to capacity for introducing harm. If these activities are evaluated using cyber-RAT it is apparent that each one may place the user as suitable

target. If a capable guardian is not present in the form of antivirus, security updates or an awareness of internet harms, victimisation may occur in the form of malware or other nuisances. A device compromised by malicious code will then become an instrument to extend the reach of an attacker and the user takes the role of unwitting accomplice. Routine interaction and further absence of guardianship can allow harm to be shared with other suitable targets in the workplace, for example, devices and digital systems used by colleagues.

The concept of fluidity was proposed in Chapter Two (2.7.1) to define how the roles of offender, target and guardian may be interchangeable when using cyber-RAT. To illustrate, consider the employee using a personal device to undertake digital activities known to be potentially unsafe. In this example, the user is both the target of the attacker who placed malware on a web page and the guardian who can prevent access to the malware. Failure to recognise the threat, lack of regular updates or no antivirus are absent guardians. The consequence may be a compromised device and the user becomes a victim. When the device is later brought to the workplace, the victim becomes the extended reach of the attacker, the suitable target is the corporate network, and the user may again become the guardian with ability to prevent any further victimisation.

Fluidity can be explored further using behaviours observed in the sample to illustrate the concept. A user may choose to forgo device security mechanisms but by visiting websites with the potential for internet harm they become a suitable target. If their device is compromised, the user takes the role of offender when the device is brought to the corporate space. Once inside the workplace, the

compromised device becomes the instrument of attack, and the user assumes the role of guardian. Routine workplace activity may require connection to the corporate network or interaction with other devices and these become suitable targets. In the absence of awareness that a device used for unsafe activity may be an offending item, further victimisation might occur.

9.6.2 Cyber-RAT and Bespoke Training

The results have confirmed a requirement for training and awareness raising amongst corporate personnel as recommended by the literature (Furnell and Clarke, 2009; PwC, 2018; Warkentin and Willison, 2009). Ideally, employee training should be fundamentally linked to personal use of technology (Rughiniş and Rughiniş, 2014) and associate personal digital activity with the potential for victimisation of self, family, colleagues and employers. To relate personal use with potential victimisation, the employee must have capacity to recognise when specific activities place them in a vulnerable position. The theoretical examples described above in 9.6.1 indicate how the cyber-RAT framework might assist with recognising suitable target and identifying opportunities for guardianship. If incorporated into employee training, cyber-RAT may provide a simple assessment tool to evaluate personal digital activity and enable user-guardianship.

To instigate an evolution of policies and procedures, organisations may require a solution of “accommodation” which is acceptable to all, regardless of conflict in points of view and opinions (Checkland and Poulter, 2007, p. 55). As an example, it may be impossible to ‘forbid’ an employee with extensive technological expertise from using personal knowledge to enhance productivity. A resolution to

accommodate perspective of security and IT management, risk assessors and the employee will involve compromise from all parties to reach a solution which everyone “can live with” (Checkland and Poulter, 2007, p. 55). Cyber-RAT may assist in clarifying where guardianship solutions may be found, and the organisation might choose to provide quality antivirus solutions free of charge and take responsibility for maintenance. In return, an employee-as-guardian may modify unsafe behaviours but continue with personal digital activity if it enhances productivity.

Employees may benefit considerably from an enhanced understanding of their role in preventing victimisation from cybercrime since lacunas in knowledge are absent guardians. Respondents who do not accept updates to systems or apps may be disturbed to learn that a lack of risk awareness had failed to make safe a recently found vulnerability. Empowered users may become the most capable of guardians with capacity for intervention if the organisation becomes suitable target. A very simple example may be preventing a device showing pop-up windows from accessing the network, since ‘pop-ups’ may be a harmless annoyance but have also been known to place malware and might be a potential threat (Newman, 2018). To place empowered guardianship into practical perspective, during the methods detailed in ‘A New Direction’ (Chapter Six), a company director who had received a letter of invitation emailed the researcher to remark on the relevance of the research topic. Prior to completing the questionnaire, the director had never considered mobile devices as a risk vector, and the survey highlighted a requirement for improved cyber-security at his

organisation which he intended to address. In this example, empowering the user to recognise suitable target had enabled capable guardianship.

In digital activity, the user may not be the only guardian capable of preventing victimisation. Using cyber-RAT to evaluate a specific web-based activity may highlight multiple sentinels to be employed to assist, alongside knowledge of where they may be found and the methods to activate them. For example, Facebook, Twitter, LinkedIn, Instagram and other social networks have controls to prevent other users from outside a network from viewing personal information. As described in 2.6.1, these controls are examples of privacy enhancing technologies (PET) and cyber-RAT recognises them as guardians. An account holder has always had the choice to make a profile publicly accessible or to select who can view content. Activating privacy controls is not difficult, although inexperienced users may find it challenging to locate them without guidance. To assist, social networks provide additional guardianship in the form of an online help centre and/or a community forum to answer questions. Evaluating social media using cyber-RAT will identify that a social network has guardian capability with capacity to prevent unsolicited viewing and (possible) abuse of content.

Active guardianship in social networking was observed during the practical research in Chapter Five, ‘Executive Risk’. It proved impossible to locate personal social media content if users have protected media profile pages with privacy controls, and in addition to capable guardianship demonstrates robustness of privacy enhancing technologies when applied correctly. Only when others in the network were lax in their application of privacy was it possible to obtain the data

required to create a convincing targeted attack. Every social network user may be a capable guardian, as they have capacity to protect their own accounts, and the accounts of everyone else in their network.

9.6.3 Cyber-RAT and Threat Intelligence

In addition to empowering user-guardians, the cyber-RAT framework may be employed as a tool to assist organisational threat intelligence by identifying average user routine digital activities with greatest potential to cause victimisation. Cyber-RAT recognises that an activity capable of victimising a user has 'fluidity' and an organisation may become suitable target for a compromised device now representing an attacker. Threat intelligence may be augmented by associating contemporary mobile threats identified by security researchers with actual behaviours conducted by mobile device and internet users. This follows the model used in the analysis (Chapter Eight) to apply the literature to evidence that devices used for personal activity are present in the workplace. In Chapter Two (2.6.1), the concept of privacy enhancing technologies (PET) was considered in the context of user-enabled PET as a method of privacy preservation taking the role of capable guardian. The issue of user-privacy should additionally be considered in respect to bespoke awareness training and the suggestion that risk assessors or security managers would benefit from an understanding of employee use of personal technology. The proposal for bespoke training does not suggest that risk managers insist on *physically* examining an employee's device(s). Instead, a dialogue could be initiated where employees may confidentially discuss how personal technologies are used and the type of applications downloaded to devices. Nonetheless, some users may already utilise technological or alternate

methods of PET (Danesiz et al., 2014; Domingo-Ferrer and Blanco-Justicia, 2020; Office of the Privacy Commissioner of Canada, 2017; The Royal Society, 2019b) and as user-guardians may consider an evaluation of their personal technology to contravene their right to privacy. An open and transparent discussion of the holistic approach to corporate security might assist personnel to recognise they are of equal value to technological systems; but an employee may continue to disengage from discussion and withhold information regarding personal digital activity. Thus, risk or information managers might decide that device use per se may be an unmitigated security risk and the organisation take responsibility for guardianship. Subsequently, cyber-RAT may assist with identifying guardianship measures to assist in essential security without undermining a users' right to privacy. The framework might additionally benefit those who assess organisational risk for CBEST intelligence-led testing (BoE,2020) (see 3.2). A multi-national organisation with thousands of personal devices accompanying employees into the workplace may find a theorised cyber-RAT evaluation highlights risk factors not typically identified during traditional threat assessment.

9.7 Augmenting the Traditional Model of Insider Threat

RQ1 actual/perceived risks aimed to ascertain *actual* risk posed by employees within the financial workplace and confirm that personal technologies and 'unsafe' behaviours may augment the traditional model of insider threat seen in the literature (Furnell and Clarke, 2009; Liang, Biros and Luse, 2016; Saxena et al., 2020; PwC, 2018; Warkentin and Willison, 2009). Evidence of personal technology as a contributor to insider threat has been presented throughout the analysis chapters and critically evaluated during the discussion. Three further

additions will be considered in 9.7 and may interest risk and security managers due to probable access to corporate networks and critical assets.

9.7.1 Personal Digital Activity using Company Issued Devices

Although the focus of the study was to identify use of personal technologies, results reveal that thirty percent of the sample conduct digital activity in the workplace using company issued devices (see 8.2). Organisations provide access to a range of devices including smartphones and tablets, but most of the company issued machines used by employees are laptops and static desktop computers (see Figure 22, 8.2.1). Devices with larger screens are suitable for a variety of computing purposes but in the office environment may be used for compiling documents and spreadsheets. They may therefore be running software favoured as soft targets by criminals, and the practice of downloading software updates may constitute an actual risk (3.3.2). Not only in respect of the 'shadow' infrastructure impeding enterprise security solutions (3.9.7) but due to the criminal trend for placing malicious code into a legitimate update so that malware is introduced into a corporation. Attacks against packages such as Microsoft Office can swiftly compromise many computers and are effective against "well protected organisations" when other methods have failed (Symantec, 2018, p. 43). Assailants may target a specific sector by compromising specialised programmes known to be used within the industry (Symantec, 2019, p. 43; The Associated Press, 2019). An example with topical relevance to the financial sector sample is an attack which compromised accounting software (ENISA, 2017, para. 3; Symantec, 2018, p. 43). Assaults against software are difficult to identify as the update is downloaded from an organisation-approved supplier (Symantec, 2018,

p. 44) or may use an authentic security certificate (Newman, 2019b). Thus, an employee responding to an onscreen prompt advising an update installation may unwittingly install malware.

In respect to **RQ1 actual/perceived risks**, personal digital activity is an actual risk as enterprise devices intended for work purposes are likely to have access to the company network and/or critical files and corporate data. Figure 23 (8.2.2) and Figure 24 (8.2.2) illustrate that employees are using company devices to engage in activities discussed throughout this work as 'unsafe'. These include gaming and streaming, identified as potential attack vectors in sections 7.4 and 9.3.4, and downloading apps with the associated risk of introducing malware in disguise (7.4). Social networking is the most popular activity, with potential to expose a digital system and subsequently a network to malware and other nuisances described in 3.4.3. (Mis)use of corporate digital property for personal activity may therefore be an insider threat comparable to the disgruntled, inefficient or vindictive employee discussed in the literature (Furnell and Clarke, 2009; Saxena et al., 2020; Punithavathani et al., 2014; Ring, 2015; Warkentin and Willison, 2009).

9.7.2 High-Ranking Personnel and Executive Privilege

A further area of interest associated with **RQ1 actual/perceived risks** and sufficient to augment the insider risk model is the issue of executive and senior employees. The largest dataset using company devices are executives and senior managers (see Figure 23, 8.2.5), whose personal digital activity includes using entertainment apps and accessing social media. Senior personnel may

consider that policies are in place to prevent employees from time-wasting or accessing harmful content and that senior status grants them extra privileges with internet and social media use. Those in high-ranking positions may spend extra hours in the office and subsequently use the company device they are working with for an occasional brief distraction. Directors who are also business owners may feel that as the company is their own personal enterprise, they are entitled to take liberty with company devices and the internet. Nonetheless, senior-level personnel are likely to have access to corporate data and other critical assets. Furthermore, it may be assumed that seniors would have more awareness of cyber threat to the financial industry and the corresponding BoE recommendations (BoE, 2020) for CBEST intelligence-led testing (see 3.2). The findings suggest that high-ranking personnel have an overall lack of awareness of contemporary cyber-threat and a failure to consider digital activity and mobile devices as an attack vector.

Results illustrated in Figure 26 (8.2.6) provide evidence that high-level personnel download software updates and apps for work and personal use. In an enterprise with no designated IT department, senior staff may conduct maintenance of digital systems, for example, productivity software licenced to the owner or organisation. Hence, the results may reflect an executive in a small corporation required to download software updates and apps for work purposes. This further highlights the potential risk to an organisation of accessing a compromised software update and introducing malware into the network. An average-user executive without specialist training in IT may be unfamiliar with contemporary attack vectors and unlikely to consider compromised software when responding to (an apparent)

authentic prompt to install an update. In a larger enterprise with a designated IT department or assigned system manager, update installation is likely to be the responsibility of a technician. In the context of **RQ1 actual/perceived risk**, senior staff downloading updates and applications for work and personal use without authorisation may be indicative of shadow IT in the workplace (see 3.9.7) in addition to the risk of accessing a malicious update.

Figure 29 (8.8.3) illustrates that the largest percentage of personal device users connecting devices to the network are executives, directors, and business owners. The findings therefore suggest an absence of policies advising best practice regarding digital activity in the workplace, or if policies are in place, high-ranking personnel may not be abiding by rules governing other employees. This again emphasises a need for bespoke training and awareness on a corporation-wide basis. A holistic approach to organisational security can only succeed if all members of the workforce are included and educating employees to be user-guardians may be futile if high-ranking staff are conducting 'unsafe' activities. Furthermore, CBEST threat intelligence may be augmented by consideration of senior and executive personnel as contributors to the threat of harm. This may be particularly relevant considering the significant number of executives (fifty-four percent) who are iOS users and the observed attitudes to device security and assumed guardianship as a risk factor discussed previously in 9.5.3 and 7.6.3.

9.7.3 Enabled Guardianship as Risk

To a risk or security manager, any employee demonstrating poor practice in protecting devices and systems may be an obvious indicator of risk. Guardianship

has not been enabled and cyber-RAT suggests that victimisation may occur. Nonetheless, enabled guardianship may additionally imply a risk factor. Use of antivirus and regular updates implies awareness of harm and methods of prevention. Thus, the average user may be satisfied that device protection has been achieved. The assurance of safety may then allow complacency to influence routine internet activities. An example of respondents who may be indicative of an over-reliance on enabled guardianship are RN17, an iOS user and RN24, who uses antivirus and is consistent with updates. In regard to the central investigation, RN17 and RN24 conduct extensive potentially 'unsafe' activity in personal space. Both respondents additionally stated they would 'Always' conduct digital activity including social media, downloading apps, gaming and streaming in the workplace whilst devices are connected to the network. The nature of their activity suggests that assumption of protection acts as reassurance and is thus contributing to extensive internet use. In the context of **RQ1 actual/perceived risks,** personal digital activity and connecting to the network is an *actual* risk. In accordance with **RQ2 average usage/impact**, the concept of a protected device is inciting unsafe activity with the capacity to harm a network.

Unless an average user has a particular interest in cyber security, it may not be understood that technological preventative solutions can be breached by sophisticated malware. Cyber-criminals consistently modify code to ensure that it retains value as an attack method (Oerting, 2016, cited in Ashford, 2016) and 'zero-day' and polymorphic malware can evade detection (Drew, Hahsler and Moore, 2017; Tran et al., 2016). Additionally, attackers will combine multiple methods into a single assault (Webroot, 2019, p. 20) to increase the chance of

successfully compromising a system. Individual bespoke training would provide opportunity to address complex attack methods and those capable of circumventing traditional defence mechanisms. Incorporating cyber-RAT into awareness training may equip those who already enable protective mechanisms with additional benefit of recognising suitable target. The empowered user may then opt to avoid additional risk to a favoured device and modify or cease the 'unsafe' activity.

The discussion relating to personal devices and digital activity is now concluded. Chapter Nine will return to the Internet of Things to elaborate further on key findings highlighted by the data with relevance to **RQ3 IoT unexplored risk.**

9.8 The Internet of Things (RQ3)

RQ3 IoT unexplored risk centred entirely on the Internet of Things with the objective of confirming whether consumer devices are present in the financial workplace and theorising the potential for harm to a network. The concept of IoT virtually present as a control app on a user's smartphone and physically present as a device worn or taken to the corporate space was to be explored. The literature in 3.11.4 emphasised the varied security risks ranging from poorly configured code, limited capacity for robust security, layers of potentially vulnerable IoT infrastructure and command-and-control apps lacking secure cloud connections (Barcena and Wueest, 2015; Bertino and Islam, 2017; Miorandi et al, 2012; Safaei Pour et al., 2019; Spiezle, 2016; Yu et al., 2020). Thus, potential for workplace harm would be theorised according to employee behaviours evidenced in the data.

Results from the IoT survey were recorded in 8.7 and 8.8 and findings show that not all respondents are smart technology users, confirming literature which suggests that consumer devices have not yet reached the ubiquity predicted by industry experts (Daly, 2016; IoT for All, 2020; Landman, 2019; The Internet Society, 2019; Titcomb, 2016). Nonetheless, the seventy percent who incorporate IoT into daily use range from individuals with a single wearable device to enthusiasts with multiple devices and systems. Forty-one percent of the devices used by respondents are fitness trackers suggesting that users enjoy the benefit of monitoring personal health and activity and the ability to adjust diet or exercise accordingly. The literature identifies a growing trend for innovative person centric IoT objects, for example, a yoga mat calibrated to a user's body (Smartmat, 2018) and socks for runners to record speed whilst comparing performance from different shoes (Sensoria, 2014). These devices (or similar) may appeal to those with interest in monitoring and measuring real time performance; inciting users of fitness trackers to invest further in IoT.

If a novelty device becomes indispensable and is of a size to be portable, then potential risk is that more devices might accompany the user to the workplace. Using the yoga mat and socks to place the relevance to **RQ3 IoT unexplored risk** in perspective, devices may enter the workplace in transit if the employee intends to use them at a class or gym after work. Alternatively, the employee may stretch or run during designated breaks and the device may be connected to the network to access the data collected during exercise. Once a device has been configured to access the network it may automatically connect next time the network is in range (Ptsecurity, 2017). Thus, a device in transit may contribute to a shadow

network (Russell, 2016). An additional concern in relation to **RQ3 IoT unexplored risk** is that security managers may be unfamiliar with the progressive innovation of IoT, and not realise that devices which do not resemble typical 'smart' units are entering the workplace. This further highlights the requirement for bespoke training, not just for the benefit of the employee who may be advised about the necessity for updates and strong passwords, but also as a two-way knowledge exchange. Risk managers will remain abreast of IoT trends, in addition to learning what devices are accessing the network.

Table 18 in 8.7.4 illustrated examples of combined multiple devices and systems, often referred to as an "ecosystem" (Kemper, 2018b, part 1) consisting of multiple wirelessly connected components. To illustrate using respondent data, RN18 owns four independent systems providing music, heat, light and surveillance. If the systems are visualised in the context of the home environment, RN18 is likely to have temperature and light controllers, infra-red cameras, lightbulbs and music speakers throughout his living space, all connected to the home Wi-Fi. The components of each system can be overseen as one autonomous unit or independently, using the control app downloaded to a device, most usually a smartphone. RN18 confirmed that his iPhone contained all the apps for the IoT systems in addition to apps accompanying a smartwatch and a voice activated virtual assistant.

A contemporary smartwatch incorporates capacity to control IoT devices, but software produced by assorted different vendors is often incompatible. Attaining a seamless connection to other devices is problematic (IoT For All, 2019), requiring

devices to be reconfigured (Kemper, 2018b, part 3) and may be beyond the capability of average users (Shylenok, 2018, quoted in Kemper, 2018b). Nonetheless, users with advanced technological skill may be capable of successfully reconfiguring devices. To explain with context, four respondents who own multiple IOT units and systems also own a smartwatch and claim to have excellent, advanced or expert technical skills, suggesting they may be above average in technical capability. This includes RN18 who claimed expert level ability in all aspects of computing and affirmed that his smartwatch was always worn in the workplace and connected to the corporate network. Although results cannot confirm it as the research instrument did not capture relevant data, RN18 may be a highly skilled enthusiast with capacity to configure IoT to be controlled from a wrist-worn device and subsequently introduce further unexplored risk to the corporate network.

The literature recognises that developments in technology will inevitably produce risk (Adam and van Loom, 2000; Beck, 1992; Beckstead et al., 2014; Orman, 2013). As more employees enter the workforce from post-millennial generations, technical ability will undoubtedly increase to include many expert level average users and this may coincide with the anticipated expansion in IoT (White, 2019; Statista, 2020c). The millennial demographic is renowned for an enthusiastic response to new technologies (Kapuria, 2008; Otey, 2013) and has proved to be early adopters, for example of contactless payments (Visa Europe, 2018). The literature predicts that millennials with decision-making status will introduce more *mobile* technologies into the workplace (Whittle, 2020) but a further consideration may be that young executives with expert technological skills will be the first to

embed emerging technologies into current workplace systems. In respect to **RQ3 IoT unexplored risk,** average users without the necessary acumen may be pushed to engage with complex systems known to have capacity for risk.

Risk managers may therefore benefit from an awareness of technical competence of personnel in addition to their affiliation with smart devices. RN18 is the perfect example, an expert-level millennial in an executive position with enthusiasm for smart technology. As innovative IoT flourishes and becomes essential to individual lifestyle, employees with technical aptitude may have ability to configure devices to join existing ecosystems, controlled from devices worn in the workplace. Shadow IoT is already recognised as the occurrence of unknown IoT devices connected to a corporate network (Russell, 2016). In the context of **RQ3 IoT unexplored risk**, unknown IoT connected to other unknown IoT may be an additional threat which increases as new technology emerges.

IoT appliances exemplify smart technology which may appear virtually or physically in corporate space. A smart coffee pot may be physically present in the office and a robotic hoover located in a users' home might be accessed remotely (and therefore virtually) using an app on a smartphone. IoT devices have been found to have poorly configured apps (Junior et al., 2019), and accessed remotely or whilst in the workplace using a smartphone connected to the corporate network may constitute a threat to the IT infrastructure. Appliances are yet another example of potential risk which may expand as new and imaginative devices emerge and individuals with no current requirement for IoT products are tempted to invest. To illustrate using contemporary devices, an intelligent houseplant

watering system or pet feeding station (IoTlineup, 2020) may interest consumers who previously considered IoT unsuited to their lifestyle. Once a device becomes indispensable, the possibility arises that a user will either access the device from the workplace, or that it may become a fixture of the office.

Thirteen respondents own IoT appliances, but crucial data was not captured by the questionnaire as users were accidently filtered from the IoT survey without opportunity to answer questions relating to workplace access (see 9.2.1). The results cannot confirm whether appliances are regularly brought to the office, are based in the office or accessed by app during working hours. To explain, RN22 confirmed ownership of an IoT kettle. This appliance is portable and confirmation of the kettle in the workplace and connected to the corporate network would have been of real value. In accordance with **RQ3 IoT unexplored risk**, results are sufficient to confirm that employees own IoT appliances and may be contributing to Shadow IoT. Low budget appliances may be a particular concern since manufacturer priority is for devices to reach market with haste rather than with capacity to manage the threat landscape (Britton, 2016). Vendors lacking resources use libraries of open-source code which may contain vulnerabilities (Wang et al., 2019) and devices may lack capacity for robust security (Safaei Pour et al., 2019). To compound the issue, users are not proactive at device security, assume that safety mechanisms are built in (Harris Interactive, 2019; Minister for Digital and Broadband, 2020), and often retain factory issued passwords leaving a device vulnerable to attack (Anderson, 2019; F-secure, 2019; Microsoft, 2019).

Legislation to ban use of default passwords (Warman, 2020) and provide advice about security and ongoing support (Gov.UK, 2019) may increase the cost of premium devices. Nevertheless, it is probable that competitive global manufacturers will continue to produce IoT for all budgets and online marketplaces may facilitate distribution and purchase. Low-cost units are likely to continue using less vigorous security measures than expensive branded models and small devices will have limited processing capacity. An additional issue may arise when new models with government approved safety standards appear, and old models are sold on. It may be possible to regulate devices sold at public auction, but private sellers or donated devices may entail that pre-legislation IoT remains in operation.

Security researchers have observed “billions” of attacks against IoT (F-secure, 2019, p. 1). Hence, a surge in IoT popularity when voice control becomes mainstream, lack of robust security in innovative low budget and small units, smart units in transit or IoT connected and controlled by IoT may all be future threats against a corporate network. Results confirmed that employees are already accessing IoT systems from the workplace and habitual access can only increase as more objects become ‘imperative’ to user lifestyle. Constant interaction with home systems and appliances and monitoring of real-time health and fitness data may reflect on employee productivity in addition to introducing continuous variable risk throughout the working day. An influx of IoT and apps may require workplace IoT policies to insist that only devices with capacity for inbuilt security are permitted on company premises. Risk and security managers may be required to ensure that IoT is purchased from reputable manufacturers and of sufficient cost

to warrant robust security. Low budget devices or those from unknown or small manufacturers may require additional policies governing workplace use or even exclusion from the workplace. Once again, bespoke awareness is suggested as a knowledge exchange. For example, users who received gifts of IoT may have no knowledge about quality or security features and a tailored session exploring safety of a particular device and the potential for harm may educate both user and training provider.

9.9 Conclusion to Discussion

Chapter Nine has discussed limitations in the survey, absent data in the results and debated whether respondents chose to pass questions which might have provided crucial data. Data gaps have affected evidence quality, but analysis of key findings have sufficiently answered the research questions, confirmed actual risk from employee behaviour (**RQ1 actual/perceived risks**) and theorised risk from use of personal technologies (**RQ2 average usage/impact** and **RQ3 IoT unexplored risk**). The results have been reviewed in the context of awareness-raising and elements of potential interest to security stakeholders have been suggested to improve cyber-awareness. Bespoke training has been discussed alongside the proposal of applying the cyber-RAT framework to demonstrate how cyber-specific routine activity theory might assist with assessment of small-scale technological risk. The concluding discussion of the Internet of Things evaluated the technologically competent employee and engagement with smart technology in the context of contemporary work-based risk. Future IoT threat in conjunction with developments in emerging devices has additionally been theorised in accordance with **RQ3 (IoT unexplored risk)**.

The critical evaluation in Chapter Eight and discussion throughout Chapter Nine illustrate that gaps in the literature (see 3.13) have been addressed. Surveying employees as a sample demonstrates that routine digital activity, personal technology, employee use of corporate digital property, current and future use of consumer IoT, executive privilege and assumed guardianship as risk may augment the current model of insider threat (see 3.2.1). These are offered as original contributions to knowledge and will be given robust consideration in the final chapter (Chapter 10). Further areas of contribution are seen in the three methodology chapters ('The Corporate World', 'Executive Risk', and 'A New Direction'). These provide insight of digital investigation which may be of value to other researchers seeking a purposive sample. The framework of cyber-specific routine activity theory (see Table 2, 2.7.4) as a theoretical model to address small scale technological risk may be a significant contribution to risk managers and policy makers. Most importantly, the reluctance observed amongst financial organisations to participate in topical and relevant research indicates an apparent failure by the sector to prepare for small scale variable and dynamic risk (see 10.3). The findings have confirmed, denied and modified the literature, and the limitations discussed in 9.2, 9.3.4 and 9.3.5 illustrate how interpretivist knowledge acquisition may be improved by other researchers. The final concluding chapter (Chapter Ten) will present the findings as the answer to the research questions (see 10.2) and offer original contributions to enhance the knowledge base in the field of corporate workplace risk management (see 10.3).

Chapter Ten: Conclusion

10.1 Introduction

The aim of this research was to establish actual and unexplored risk introduced by employees and digital behaviour and ascertain unknowing or inadvertent (mis)use of personal technology as a contributory factor to human-assisted cybercrime. Despite societal dependence on online resources, typically accessed via a mobile device, literature evaluating average-user employees and routine technology use as a workplace risk is lacking. Regardless of the ubiquitous presence of 'smart' technology, employee use of person-centric or consumer IoT devices in and out of the workplace has not yet been addressed as a risk factor. To achieve the research objective of assisting financial corporations to reconsider employees as an insider threat by contemplating technological lifestyle and contemporary culture, the study aimed to answer the following three questions.

- **RQ1 (actual/perceived risks).** What are the actual rather than the perceived risks created by personnel within a financial organisation?
- **RQ2 (average usage/impact).** How does an average user utilise their own mobile device(s), and how may this impact on the corporate IT infrastructure?
- **RQ3 (IoT unexplored risk).** Are devices and applications associated with the emerging Internet of Things establishing a presence in the workplace and what unexplored risk might this entail?

The conclusion chapter is arranged as follows: empirical findings are examined in 10.2 beginning with **RQ1 actual/perceived risks** (10.2.1) and confirmation of the employee as an actual risk beyond the current perception of deliberate or

inadvertent harm (Liang, Biros and Luse, 2016; Mouton et al, 2014; Saxena et al., 2020; Warkentin and Willison, 2009). This is followed by **RQ2 average usage/impact** (10.2.2) revealing the potential for threat created by personal technology and **RQ3 IoT unexplored risk** (10.2.3) with evidence of virtual and physical consumer IoT and the threat to a network. An original contribution to knowledge is offered in 10.3 and the synthesis of empirical evidence enhanced by the methodologies and key observations from the results propose a revaluation of the employee as a risk to the organisation. 10.4 addresses limitations and 10.5 will recommend areas for further research. 10.6 offers a brief reflection on the overall outcome and will conclude the thesis.

10.2 The Findings

Chapter Two established the theoretical framework at the core of the project. Fundamental elements of suitable target, motivated offender, and capable guardian from the crime prevention model of routine activity theory (RAT) (Cohen and Felson, 1979) were augmented with liquid modernity (Bauman, 2000). This reimagining of RAT (2.7.3) was then transposed to the digital domain to become a cyber-specific framework for evaluating technological behaviours of financial sector employees to define risk of convergence in the absence of guardianship. **RQ1 actual/perceived risks** would evidence employees as an *actua*l risk due to digital activity, regular internet use and passive and active footprints (Azucar, Marengo and Settanni, 2018; Madden et al., 2007; Micheli, Lutz and Büchi, 2018). **RQ2 average usage/impact** and **RQ3 IoT unexplored risk would** *theorise* risk arising from regular activity using personal technologies. Literature discussed in Chapter Three argued that the internet is a serious threat with capacity to share numerous and varied harms to users, devices, and networks (Burns, Johnson and

Caputo, 2019; Drew, Hahsler and Moore, 2017; Emm, 2020; McMillan, 2010; Qamar, Karim and Chang, 2019; Razak et al., 2016; Sood and Enbody, 2011). Applying cyber-RAT as a tool during digital investigation to identify a purposive sample provided findings to satisfy the requirements of actual and theorised risk.

10.2.1 Research Question One

A reappraisal of Research Question One from the theoretical perspective of cyber-RAT determines that actual risk sought by **RQ1 actual/perceived risks** addresses potential convergence of a suitable target facilitated by digital footprints and enabled by absent guardians. Chapter Four, 'The Corporate World' demonstrated how user-generated footprint and suitable target are inextricably linked without enabled guardianship of privacy. The chapter confirmed that frontline and entry-level financial employees provide accessible content to achieve credibility for phishing attacks. Social media users were observed with narcissistic traits (Bergman et al, 2011; Carpenter, 2012; Wang, 2017), posting self-promoting user content and images intended to invoke comment from the online audience (see 4.10). **RQ1 actual/perceived risks** finds digital narcissism (Lovink and Rossiter, 2009) may equate to suitable target, as accessible data may facilitate actual risk of targeted attack. This is reinforced in Chapter Five, 'Executive Risk' where observed behaviours of financial executives displaying narcissistic qualities enabled collection of data suitable for social engineering (see 5.4.3). Passive and active online content, photographs and heritage data from archived resources can initiate suitable target for focused exploits in regard to **RQ1 actual/perceived risks**. Chapter Five confirmed that high-ranking personnel might act as a 'gateway' to an organisation or colleague with value to an attacker and may be an

actual risk of convergence as sought by **RQ1 actual/perceived risks**. Chapter Six, 'A New Direction' identified **RQ1 actual/perceived risks** in personal data published as employee biographies on corporate websites. No open-source intelligence was required to identify suitable target as company-generated active footprints may place a corporation at risk of targeted attack.

Employees from all levels of corporate hierarchy, including senior and executive personnel with assumed responsibility for critical assets employ company-issued devices for personal use. **RQ1 actual/perceived risks** is seen when employees place enterprise systems as suitable target at risk of convergence from malware and other internet harms. Digital activities recognised as potentially 'unsafe' (Ashford, 2019; Bode, 2018; Cullen, 2018; Cuthbertson, 2019b; Deloitte, 2019; Lutrum, 2019) including streaming, gaming, and usage and download of apps routinely take place in the financial workplace. System upgrades and software downloads which may be under remit of qualified technicians are undertaken by average-user employees. **RQ1 actual/perceived risks** identifies risk of malware disguised as genuine software entering systems with access to critical data (see 9.7.1). Procurement of apps and software may additionally be indicative of a shadow IT infrastructure occurring in the workplace without the knowledge of IT managers (Carter, 2015; Chapman, 2015; Froehlich, 2015).

Chapter eight confirmed **RQ1 actual/perceived risks** as respondent data showed social networking taking place using company issued devices. Employees throughout the corporate hierarchy threaten corporate networks with a vector known to share malware and other nuisances (Ashford, 2019; Sood and Enbody,

2011). Employees routinely generate active digital footprints (Madden et al., 2007) from user-generated content typical to that used during the digital investigation (see Chapter Four, 'The Corporate World' and Chapter Five, 'Executive Risk'). Respondents confirm that data of value to an attacker is available on social network profiles and guardianship in the form of enabled privacy is inconsistent (8.5). Narcissistic tendencies were evidenced in respondent behaviours (8.5.6) and for **RQ1 actual/perceived risks**, the average-user employee-narcissist may generate abundant personal data unprotected by guardianship. Easily identifiable images and self-promoting content where other users leave key data as comments may invite risk of targeted attack (5.4.3).

Substantial use of communication and messaging applications in the workplace demonstrates **RQ1 actual/perceived risks**. Employee use of WhatsApp despite apparent vulnerabilities (Amit and Gat, 2019; Blanco, 2020; CisoMag, 2020; Lee, 2019; Newman, 2019a; WhatsApp, 2020; Which, 2020) may indicate an actual risk of malware infection, particularly if communication apps are downloaded to company devices and used to share corporate files or data between colleagues. Results confirm that technological behaviour places the employee, and by association the organisation, in position of suitable target. Corporate issued devices utilised for 'unsafe' personal digital activity, use of social networks and communication technologies in the workplace, average-users undertaking system upgrade and unprotected personal data available online may all be considered as an actual risk in the context of Research Question One.

10.2.2 Research Question Two

Theoretical cyber-RAT defines Research Question Two as routine activity where a user may become suitable target through ‘unsafe’ use of personal technologies, and convergence with an offender or instrument (see 2.3.1) might occur without enabled guardianship. **RQ2 average usage/impact** was first suggested in Chapter Four, ‘The Corporate World’ where self-portraits and other self-promoting content posted to social media by ‘narcissistic’ users were photographed from inside the workplace (4.8.5). As ninety-nine percent of social media users conduct activity using mobile devices (Statista, 2020b), images posted to social spaces are likely to have been produced using personal technologies. Routine use of devices to generate unprotected content of value to an attacker is a theorised risk. Chapter Seven analysed respondent data relating to personal technologies to conclude that multiple devices used for personal digital activity (see 7.3) are brought to the workplace and connected to corporate networks. In Chapter Eight, the cyber-RAT framework in association with academic and cyber-security literature theorised suitable target and absent guardianship in the context of workplace risk. **RQ2 average usage/impact** is indicated by employees throughout the corporate hierarchy routinely using apps to engage in potentially ’unsafe’ activity, including streaming, games, adult content, social media, gambling and communication (see 7.4) and the security implications of malicious, outdated or unpatched applications (Guerra, 2015; La Porta, 2018; McAfee, 2019; Symantec, 2019). Other evidence of **RQ2 average usage/impact** is indicated by employees ‘unsafe’ activity in personal space which may be continuing in the workplace whilst a device is connected to the network (8.3.2). Users are inconsistent with security updates and use of technological prevention systems

(see 7.6). Absent guardianship may allow malicious harm to spread via application use. Unsecured apps installed to devices may compromise a device connected to the network, allowing access to critical data or corporate assets.

Results confirm that social media is accessed in and out of the workplace using personal devices and employees have profiles on multiple sites (8.5). Social platforms are known to spread harm (McGuire, 2019; Sood and Enbody, 2011) (see 3.4) and are an acknowledged risk to corporations (Ashford, 2019; McGuire, 2019). **RQ2 average usage/impact** finds access to social media using a personal device connected to corporate infrastructure initiates suitable target, placing users and organisations at risk of convergence. Respondents suggesting narcissistic traits who publish selfies intended to invoke response from other users (Wang, 2017) may use personal devices for frequent access to social profiles to add content and review and respond to comments. **RQ2 average usage/impact** is seen in personal technologies used to contribute to user-generated content, and if the narcissistic employee has profiles on many platforms, risk of digital footprint initiating targeted attack may increase. Furthermore, frequent access to the threat-arena of social media may increase potential for convergence with an offender or instrument extending the offenders reach. **RQ2 average usage/impact** has relevance to the ubiquitous presence of message and communication applications on devices and their use in the workplace (see 8.6). Communication services have been exploited by criminals to spread malware (Anstett, 2019; Lutrum, 2019) and a compromised message sharing harm to other devices or corporate data sharded between devices affected by malware is a further theorised risk of average usage.

Chapter Nine discusses how **RQ2 average usage/impact** applies to respondents who believe a device is securely protected and subsequently practice 'unsafe' digital activity. This includes users who personally enable guardianship and those convinced of safety due to alleged security of the device they use. Of particular concern are iOS device users as results suggest a generic user-conviction of immunity to harm, despite evidence of iOS vulnerability (Golubev, 2019; Goodin, 2019; Hay Newman, 2019; Kokh, 2019; Seals, 2020; Whittacker, 2019). Executive personnel are observed to be conducting most 'unsafe' activities whilst connected to the corporate network and iPhones are the device used by many senior members of staff (9.7.2). Assumed device security instigating unguarded digital activity for those responsible for corporate assets is (9.7.3) is additionally significant to **RQ2 average usage/impact**.

10.2.3 Research Question Three

RQ3 IoT unexplored risk seeks unexplored routes to victimisation and applies the concept of guardianship to smart technologies vulnerable to virtual attack. Data was captured in an exclusive IoT survey, concealed within the research instrument and accessed only by users who confirmed ownership of smart technologies (see 8.7 and 8.8). Chapter Eight demonstrated that seventy percent of respondents own a combined total of one hundred and twenty-one (121) IoT devices ranging from a single unit to a collection of systems, appliances and wearable devices (see 8.7.2 and 8.7.3). Smartwatches and fitness-trackers are worn to the workplace, and some connect to the corporate network. In accordance with **RQ3 IoT unexplored risk,** IoT software is vulnerable to flaws (Miorandi et al, 2012) and tiny processors in wearable devices may lack adequate

processing power for robust security (Bertino and Islam, 2017; Safaei Pour et al., 2019). Command-and-control applications for IoT systems and appliances are prevalent on personal devices entering the workplace (8.8.3). IoT apps may be a security concern (Barcena and Wueest, 2015; Yu et al., 2020) and forty percent of respondents have three or more apps installed to devices connected to the corporate network (Figure 46, 8.8.3). IoT appliances may prove a current and future risk with potential for expansion as technologies become increasingly innovative (9.8). Complex IoT infrastructure may contain vulnerabilities (Miessler et al., 2019; Spiezle, 2016) and can be targeted by IoT specific malware engineered to avoid detection (Alasmary et al., 2019; Costin and Zaddach, 2018) Darabian et al., 2020; Drew, Hahsler and Moore, 2017; Masabo et al., 2018) (see 3.11.4). **RQ3 IoT unexplored risk** finds that appliances might be represented virtually by an app on a smartphone or inside the corporate space and connected to the network. A trend for 'ecosystems' (Kemper, 2018b) consisting of multiple IoT systems and devices networked together suggests potential for technologically advanced employees to reconfigure control mechanisms to command home-based IoT using a wrist worn device (see 9.8). In regard to **RQ3 IoT unexplored risk**, a tiny device with limited security (Bertino and Islam, 2017; Safaei Pour et al., 2019) used to access multiple command-and-control apps may constitute a further risk if connected to enterprise IT infrastructure. **RQ3 IoT unexplored risk** finds that users receiving IoT gifts have limited awareness of device security, and coveted devices may have been selected for compatibility with a user's lifestyle and not for robust security. In general, guardianship in the form of regular updates and changing default password is inconsistent (see 8.7.5 and 8.7.6) and relevant to **RQ3 IoT unexplored risk**.

10.2.4 Implications

Portable devices used for personal digital activity at home and elsewhere are brought to the workplace and despite apparent lack of basic security mechanisms are granted access to the corporate network. All members of the corporate hierarchy are actively engaging in activities recognised by security experts and academics as capable of introducing harms to devices and networks (Ashford, 2019; Bode, 2018; Cullen, 2018; Cuthbertson, 2019b; Deloitte, 2019; Lutrum, 2019; Sood and Enbody, 2011). The use of emerging technologies in the workplace and the presence of command-and-control applications on devices may be an unmitigated threat likely to increase as more everyday objects receive computerisation and appeal to new markets. As technologically advanced users from post-millennial generations join the workforce or gain decision-making status, additional emerging and disruptive technologies are likely to embed into current systems. Average-users with little or no affiliation for technology may be required to use increasing numbers of advanced, sophisticated and complex systems they do not understand.

The results confirm the literature and acknowledge that a holistic approach to risk management (Salim and Madnik, 2016), may be enhanced by training tailored to personal digital activity (Rughiniş and Rughiniş ,2014; Russell, 2016). In place of generic learning which can jade, alienate or appear irrelevant (Johnston, Warkentin and Siponen, 2015), bespoke instruction might enlighten a user to risks specific to personal digital activity and ideally evolve with every new technological advancement embraced by users. Dangers to self, others and corporate systems may thus be addressed dynamically, in conjunction with progressive changes in

user activity. Cyber awareness can become outdated as threats and harms created by new technologies are often unfamiliar. Thus, data indicative of unexpected risk accumulated during bespoke employee interaction may be shared with stakeholders. Policy makers, risk managers and corporate IT security teams may address gaps in knowledge and enhance professional practice, strengthening enterprise security accordingly.

10.3 Contribution to Knowledge

This thesis offers several individual elements of original contribution. The novel theoretical framework of cyber-specific RAT enables evaluation of digital behaviour to determine an average-user as suitable target and is offered as original contribution to assist with small-scale technological risk analysis. Cyber-RAT borrows from the traditional crime prevention model of routine activity theory (Cohen and Felson,1979) and has been applied in practice throughout this study. The framework assists in theorising risk arising from routine digital activity by evaluating the concept of suitable target (a potential victim resulting from use of the internet), motivated offender or instrument to extend reach (malicious code, phishing, social engineering, scams and others) and capable guardian (antivirus, privacy controls, a cyber-aware user-guardian, risk managers, site administrators, help centres, other forms of online support). The fluidity described in Chapter Two (2.7.1) facilitates visualization of how a theorised risk scenario might evolve, for example, a smartphone might be suitable target whilst an employee visits social networks, but user-guardianship may be enabled to prevent access to an 'instrument' extending reach of an offender (see 2.3.1), for example, an infected hyperlink. If convergence takes place, the device becomes an 'instrument' for the

employee who is now an (unwitting) attacker in a corporate workplace. The organisation becomes suitable target at risk of convergence unless guardianship is enabled. Fluidity allows flexible roles between players, intimating how specific actions may change outcomes and assist in resolving the underlaying cyber-risk dilemma of: how does an average user become a suitable target, and how does an average user become a capable guardian? (Hicks, 2020)

Used as an evaluation tool in the literature review in Chapter Three, cyber-RAT theorised known security threats to mobile and smart technologies as offenders/instruments, and internet users without applicable guardianship as suitable target. The framework was then applied throughout the research methods documented in Chapters Four and Five to identify suitable target in the form of employees with no enabled guardianship and financial organisations at risk due to unprotected user-generated content. The practical application of the theoretical framework was a key element during critical analysis and discussion and cyber-RAT demonstrated value as a tool to evaluate small-scale dynamic risk. The framework performs best when assisted by literature detailing contemporary cyber threat, for example, internet security threat reports (see Fireeye, 2019; McAffee, 2019; Symantec, 2019; Webroot, 2020) and is therefore suggested as an aid to enhance bespoke training and awareness. To enable guardianship, the user requires cognizant awareness to recognise where activity might be modified, ceased or additional mechanisms put in place. Cyber-RAT as a tool to evaluate individual user behaviour may not only enable employees to recognise threat of harm unique to their personal circumstances but may assist security managers to recognise where unmitigated threats to enterprise security exist.

Employee use of personal technology is offered as original contribution to augment the traditional model of insider threat (Liang, Biros and Luse, 2016; Mouton et al, 2014; Saxena et al., 2020; Warkentin and Willison, 2009). By addressing the gaps observed in the literature (see 3.13) and surveying a sample of diversely demographic financial sector employees (see 7.2), substantive evidence of digital behaviours has been collected. Findings demonstrate that personal device use may be a contributory factor to organisational risk. Digital activity where a user is *present* in cyberspace, for instance, social networking; activity which requires *facilities* of cyberspace, such as downloading applications and software; and activity using a *service* delivered by the internet, for example, streaming media, gaming and adult content, may all place a user and/or their device at risk of convergence with harms. These might take the form of a human offender attempting a targeted assault on a network, or an 'instrument' which might compromise a device and spread throughout IT infrastructure. Employees routinely using devices in personal space for activity with capacity to introduce harm (7.4) who then connect devices to corporate networks, may be considered as a potential insider threat.

Physical and virtual presence of consumer IoT in the workplace is a necessary addition to the current insider model. IoT is well established amongst financial services employees and represented physically in the workplace as wearable devices and virtually as applications on smartphones. Awareness of IoT security may be lacking despite enthusiasts embracing ecosystems of combined devices (8.7.4), and average-user employees may possess technological skills to enable reconfiguration of systems to suit personal taste (9.8). The findings imply a risk

likely to expand as IoT evolves and new technologies are incorporated into smart devices (White, 2019). Innovative units may appeal to new demographics, thus increasing the IoT user-group. Addressing network security before technologies such as voice activation and facial recognition cause consumer IOT to scale exponentially can only be advantageous to corporations.

Added value is found in results which establish senior and executive level personnel as practitioners of unsafe behaviours with presumed device security as licence for unrestricted online activity. Assumption of protection may instigate complacency toward internet use without awareness that guardianship may be inadequate to prevent convergence of target and offender. Privilege of rank may contribute to non-observance of policies and best practice. Knowledge that the upper echelons of corporate hierarchy may be a specific security risk might be of value to CBEST assessors when evaluating internal corporate threat (BoE, 2020) (see 3.2). This has particular relevance when associated with the findings of the digital investigation (Chapter Five, 'Executive Risk') which established that internet presence, social media use, unprotected content and personal networks place high-ranking staff at risk of targeted attack.

Social media users who knowingly or inadvertently make personal data accessible to a public audience may also be considered as a contributor to insider threat since unprotected content can be of value to an attacker attempting an assault on a network via a targeted social engineering attack. A social media user displaying narcissistic tendencies (Bergman et al, 2011; Carpenter, 2012; Lovink and Rossiter, 2009; Wang, 2017) offers a variety of unique threats. They publish self-

portraits, self-promoting materials, personal data and images where they are easily identifiable, and may deliberately forgo privacy enhancing technologies so that users outside their immediate network can access content and leave positive feedback. Their behaviours may be predictable, allowing an attacker to recognise that data of value will be found and accessible (see 5.4.3 and Appendix B), making them a suitable subject for targeted social engineering and use as a 'gateway' into an organisation or 'bridge' to another more valuable target. The narcissistic users desire for flattering feedback may make them vulnerable to abuse of trust by attackers attempting to infiltrate a personal network by acceptance as a friend or follower. In the context of personal technology use, a narcissistic user may have social profiles on several networks so that content will be available to different audiences. Maintaining multiple profiles and responding to comments may entail a device frequently accessing social media where it might be exposed to harm. If the device is connected to a corporate network, IT infrastructure is additionally at risk.

The three unique methodologies are proposed as original contribution, offered as 'roadmaps' to other researchers who may replicate techniques and improve upon the outcome. Each methodology provides insight of internet facilities, open-source practices, methods and possibilities enabled by online research and charts the challenge of digital investigation. Chapters Four, Five and Six illustrate how online research may not follow anticipated strategies and requires adjustment and willingness to explore unfamiliar resources to reach an acceptable solution. The research methods demonstrate how constant due diligence and a respect for ethical boundaries combined with creativity, tenacity and determination may

achieve a sample meeting particular requirements to address specific gaps in literature. Furthermore, 'The Corporate World' and 'Executive Risk' demonstrate how a methodology may be used to gauge the practical value of a theoretical framework. In respect of the research questions, data collection provided conclusive evidence of employee instigated risk and the methodologies contributed to the findings as a resource for critical evaluation.

The final offer of original contribution is presented here as a brief reflection on the search for a data sample, re-evaluated with consideration of 'question threat' (Foddy, 2011, p.117). Financial regulators and the Information Commissioners Office expect a standard of security throughout the financial sector (Kember, 2018) and the Bank of England recommends CBEST intelligence-led resilience testing (BoE, 2020) (see 3.2). The doctoral project aimed to conduct topical research relevant to a sector expected to manage the threat of cybercrime and Chapter Five, 'Executive Risk' and Chapter Six, 'A New Direction' endeavoured to engage assistance from financial corporations. Access to findings was offered on assumption that stakeholders might welcome an improved understanding of contemporary insider threat.

Approximately three hundred and sixty-four (364) key personnel from more than two-hundred and thirty-three (233) financial organisations are known to have been personally invited to participate (see 6.5). This number does not include informal requests issued by colleagues and acquaintances, nor those who may have seen the post on the website of the Midlands Fraud Forum (MMF). Despite the number of letters and emails sent to corporations, approximately eighteen (18) survey

submissions are known to have been generated from personal invitations (see 6.7). Two financial organisations who responded to the report issued at the close of 'Executive Risk' (see 5.5) and a third corporation introduced by an academic colleague (see 6.6.3.2) all offered initial support but withdrew from the project without explanation. All three had requested the research instrument and it is assumed that withdrawal was a response to viewing the survey content. Despite approval from the University Research Ethics Committee, two unrelated incidents implied that the questionnaire may be disconcerting. A colleague who tested the survey recognised poor personal cyber awareness and claimed a re-evaluation of digital activities, and a financial services respondent reported intention to review organisational cyber security. This suggests that the three organisations who reviewed the questionnaire were affected by question threat, and Foddy's (2011) theory may have prompted withdrawal of support.

Financial personnel who received personal invitations did not view the survey in advance but still declined to volunteer and it is important to clarify the reason. Invitation by letter gave option to engage with the project or dispose of the letter with no further thought. Recipients had no relationship with the researcher and could cause no offence by not responding to the invitation. At the other end of the spectrum were financial connections who were asked in person by an academic colleague with whom they had a long-standing professional relationship. Although each financial contact acknowledged interest, they refused to participate in the project. Being compelled to recognise that their financial employers may not have policies and approaches in place to counteract dynamic cyber security risks of a

small to medium scale may have caused a level of discomfort to the representatives of organisations (Hicks, 2019).

Financial corporations are **"**sensitive about cyber" with "extraordinarily little/no policy enforcement on cyber security or training" (Kember, 2018, para. 1). Fear that "their name will leak" (Kember, 2018, para. 1) and exposure as vulnerable may have caused a measure of disquiet to enterprises. In respect of this research study, the minimal response to a wide-scale invitation issued to a sector required to manage cyber-risk is a practical demonstration of original contribution. Financial organisations may not be prepared for dynamic, small-scale risk and policies for cyber security seem oriented to large scale policy and operational issues, rather than the day-to-day uses and risks from ordinary technology usage (Hicks, 2019). This further confirms the proposal that employee (mis)use of personal technology is a necessary addition to insider threat.

10.4 Limitations

The shortcomings observed in the research instrument and survey experience have already been discussed (7.2.4 and 9.2) but two further limitations affected the outcome of this study. The overall sample was so small that when themes became apparent and were explored further, each individual sample decreased in size and eventually some consisted of only six respondents. Instead of a definitive conclusion, results from tiny samples could only be indicative of user behaviours. For the purposes of the study, indication was adequate since the premise of the research required confirmation that specific activity occurs in the financial workplace, and the data satisfactorily provided that information. From a

personal perspective, the researcher could not help a sense of disappointment that the large corporations had withdrawn their offers of assistance. A substantial sample from a multi-national corporation may have provided explicitly conclusive data and irrefutable findings may have had real impact.

The second limitation is that the research instrument encompassed too many diverse areas of potentially harmful digital activity. Internet threats are numerous and variable and rather than an attempt to examine every area of digital activity, it may have been preferable to streamline data collection. A focus on one or two issues with sufficient literature to confirm a threat to device and/or user would have enabled thorough examination of user-group typology. Comparisons, differences or similarities between demographics may have been found to benefit risk assessment and security managers. Examples where a focused appraisal of users and behaviours would have been advantageous are suggested in 10.5 as recommendations for further research.

10.5 Further Research

The results demonstrated that significant numbers of respondents make use of communications applications. The data was limited regarding actual usage, and further evaluation is required to understand the role of these apps in the workplace. The potential for harm spread between users was identified during the discussion but specific data is lacking to confirm whether employees use WhatsApp or Facebook Messenger to share corporate data and work documents. Further academic work might ascertain whether use should be restricted during working hours or prevented for devices connected to the corporate network.

Findings indicated many areas of potential risk introduced by routine activity, but specific data relating to ‘sensitive’ issues was not collected. Use of apps for streaming media content, playing games and accessing adult content was evidenced in the results, but the findings demonstrate only that devices are used for these activities. The data cannot confirm genuine behaviour likely to introduce harm, thus, results cannot be used as a robust framework of user conduct of real value to risk assessors. Further research might examine whether copyright protected media, patched or cracked games (see 7.4.4) or adult content is accessed with sufficient frequency to place a device at risk of encountering malware. The parameters for this research required that infrequent (Very Rarely) unsafe activity be of equal risk to regular activity due to the nature of internet harms and the potential for random attack. A diligent examination of ‘free’ content accessed by employee devices may verify definite trends and ascertain whether certain activities should be prevented, restricted, or monitored in the workplace.

Further academic research might use targeted enquiries to examine issues which could not be explored thoroughly due to non-specific questions in the survey. In particular the use of jailbroken or rooted devices as a contemporary security threat (Symantec, 2019) in connection with employees possessing advanced technological skills to facilitate device modification. In consideration of the suggestion that iOS users may be complacent towards device security (see 7.6.3 and 9.5.3), further research might identify whether Apple devices were purchased as luxury lifestyle choices or for the ‘in-built’ security. This may confirm that the superior security of the Apple brand is a fortuitous circumstance or that iOS consumers are security conscious and made an informed decision towards

personal safety. Findings from iOS specific research may indicate that users require enhanced training to mitigate over-reliance on an imperfect system in addition to bespoke risk awareness pertaining to personal behaviours.

Further research regarding consumer IoT is recommended, in particular, use of smart appliances as those enjoyed in the home may be brought into the corporate environment for the convenience of the user. Data of value might establish whether an infrastructure of shadow IoT appliances is present in the workplace. As more objects receive sensors and voice activation technology becomes standard, novelty IoT may appear in, or pass through the workplace in transit, thus, additional work might focus on new or innovative units. Routine activities requiring an IoT device to travel may result in connection to other networks en route with the risk of spreading harm from network to network and academia may identify areas where enhanced security may be of benefit. Further research relating to IoT might consider the rapidly changing consumer landscape. Enthusiasts may purchase an upgrade whenever new models with additional features are issued, but do not remove outdated units or apps from networks or devices. Additionally, models which have not met expectation and are no longer in service may remain connected to a network either in the user's home or office. Research to establish the extent of unused and possibly unsupported devices owned by employees and the prospect of associated applications remaining on smartphones in the workplace may add value to risk assessment.

10.6 Final Conclusion

Internet culture and reliance on networked technologies ensures that average users will continue to engage with complex and sophisticated software and systems. In the current decade these take the form of handheld or body worn devices, but technological developments will not cease, and progress may take technology in unpredictable directions. Although threats of the future might differ, human behaviour and routine digital activity may not. If attackers continue to take advantage of the human weakness for 'the next big thing' as a delivery system, the average user will always be a suitable target and subsequently a potential risk.

Personal technologies have altered the traditional model of insider threat and cybercrime prevention in contemporary society requires a greater appreciation of the human factor. This may be particularly relevant in light of the 2020 novel coronavirus pandemic, and the necessary lockdowns which instigated a monumental shift in routine digital activity. This thesis demonstrated that average-user employees in the pre-Covid era use personal devices for 'unsafe' activity, but the pandemic may introduce further unmitigated risk with potential to increase as post-Covid industry instigates new working practices. During the lockdowns of 2020 and 2021, office-based staff were encouraged to work remotely, and this new system of home-working coincided with a rise in online retail and the closure of educational establishments. In addition, users from all demographics confined to their homes, relied on technologies to assist social interaction and increased usage of 'unsafe' (see 7.4) online entertainment services was observed, in

particular streaming, gaming and adult content (BBC News, 2020b; BBC News, 2021). It is entirely possible that employee owned devices were used for personal digital activity *and* shared with others for home schooling, access to study resources, grocery and domestic shopping, in addition to other users online activity. These devices were then utilised to remotely access corporate networks.

As restrictions ease, the post-pandemic employee is likely to experience working practices comprised of occasional office-based activity and continued home-working, where social media and communication technologies such as Zoom, or Microsoft Teams enable interaction with colleagues and managers. It is thus likely that personal devices will consistently access enterprise networks and despite an employee infrequently entering the physical workplace, routine digital activity and possible impact on corporate systems may be a continuous issue to be addressed by risk managers and stakeholders. Therefore, those responsible for protection of systems, customer data, critical infrastructure and corporate assets may be advised to think beyond traditional solutions and acknowledge the user-guardian as a key component in a secure organisation. Cyber-specific RAT as a practical support to small-scale dynamic risk assessment and bespoke training may assist organisations to recognise that cybercrime is not primarily a technological issue. and aid progress towards an enhanced culture of cyber awareness.

References

Ab Rahman, N.H. and Choo, K.K.R. (2015) 'A survey of information security incident handling in the cloud', *Computers and Security*, 49, pp. 45–69. 10.1016/j.cose.2014.11.006.

Abrams, L. (2019) *The hotlist is the latest Instagram phishing scam attack*. Available at: https://www.bleepingcomputer.com/news/security/the-hotlist-is-the-latest-instagram-phishing-scam-attack/ (Accessed: 3 April 2020).

Absalom, R. (2015) *Enterprise mobility: The impact of changing employee behaviour*. Available at: http://servicedeskinstitute.com/admin/includes/download.php?id=1113 (Accessed: 13 February 2017).

Aburrous, M., Hossain, M.A., Dahal, K. and Thabtah, F. (2010) 'Experimental case studies for investigating e-banking phishing techniques and attack strategies', *Cognitive Computation*, 2(3), pp. 242–253.

Ackerman, G. (2019) *Fake Facebook warlord used to spread malware, researchers say*. Available at: https://www.bloomberg.com/news/articles/2019-07-01/fake-facebook-warlord-used-to-spread-malware-researchers-say (Accessed: 3 April 2020).

Adam, B. and van Loom, J. (2000) Repositioning risk: The challenge for social theory. In Adam, B., Beck, U. and van Loon, J. (Eds) *The risk society and beyond : critical issues for social theory*. SAGE. pp.1-30 (e-book) available at: https://books.google.co.uk/books?id=MEI2iW1_E68C&pg=PA1&dq=The+Risk+society+and+beyond:+critical+issues+for+social+theory&lr=&source=gbs (Accessed: 22 February 2021).

Adewole, K.S., Anuar, N.B., Kamsin, A., Varathan, K.D. and Razak, S.A. (2017) 'Malicious accounts: Dark of the social networks', *Journal of Network and Computer Applications*, 79, pp. 41–67.

AgrafIoTis, I., Nurse, J.R., Buckley, O., Legg, P., Creese, S. and Goldsmith, M. (2015) 'Identifying attack patterns for insider threat detection', *Computer Fraud and Security*, 2015 (7), pp. 9–17.

AirBnB (2017) *AirBnB Fastfacts*. AirBnB Press Office. Available at: https://press.atairbnb.com/app/uploads/2017/.../4-Million-Listings-Announcement-1.PDF (Accessed: 12 Apr. 2018).

Alasmary, H., Khormali, A., Anwar, A., Park, J., Choi, J., Abusnaina, A., Awad, A., Nyang, D. and Mohaisen, A. (2019) 'Analyzing and detecting emerging internet of things malware: A graph-based approach', *IEEE Internet of Things Journal*, 6 (5), pp.8977-8988.

Alcorn, C.L. (2016) *How millennials in the workplace are turning peer mentoring on its head*. Available at: http://fortune.com/2016/07/26/reverse-mentoring-target-unitedhealth/ (Accessed: 25 November 2016).

Alister (2018) 'How to safely watch pirated movies, open infected files?', *Stack Exchange*, 15 July. Available at: https://security.stackexchange.com/questions/189564/how-to-safely-watch-pirated-movies-open-infected-iles#comment373964_189571 (Accessed: 8 November 2019).

Allan, D. (2019) *Windows 7 users are still refusing to upgrade to Windows 10*. Available at: https://www.techradar.com/news/windows-7-users-are-still-refusing-to-upgrade-to-windows-10 (Accessed: 29 October 2019).

Allen, D. (2020) *Windows 7 users are refusing to upgrade to windows 10 – despite Microsoft's warnings*. Available at: https://www.techradar.com/uk/news/windows-7-users-are-refusing-to-upgrade-to-windows-10-despite-microsofts-warnings (Accessed: 30 March 2020).

Alpaydin, E. (2016) *Machine learning. The new AI*. MIT Press

Amirtha, T. (2016) *Dutch police get OK to exploit zero-days: So, will that just mean more surveillance?* Available at: http://www.zdnet.com/article/dutch-police-get-ok-to-exploit-zero-days-so-will-that-just-mean-more-surveillance/ (Accessed: 7 December 2016).

Amit, Y. and Gat, A. (2019) 'Symantec Mobile Threat: Attackers Can Manipulate Your WhatsApp And Telegram Media Files,' *Symantec-blogs*, 15 July. Available at: https://symantec-blogs.broadcom.com/blogs/expert-perspectives/symantec-mobile-threat-defense-attackers-can-manipulate-your-whatsapp-and-telegram-media (Accessed: 5 April 2020).

Ammari, T., Kaye, J., Tsai, J. and Bentley, F. (2019) 'Music, search, and IoT: How people (really) use voice assistants', *ACM Transactions on Computer-Human Interaction*, 26(3), pp.1-28.

Anagnostopoulos, M., Kambourakis, G. and Gritzalis, S. (2015) 'New facets of mobile botnet: Architecture and evaluation', *International Journal of Information Security*, 15(5), pp. 455–473. doi: 10.1007/s10207-015-0310-0.

Anderson, K. (2016) 'Getting acquainted with social networks and apps: Gotta catch them all? Augmented reality gaming apps', *Library Hi Tech News,* Vol. 33 No. 10, pp. 6-8.

Anderson, T. (2019) *Even tech giants find themselves telling folk not to use default passwords on Internet of S**t kit*. Available at: https://www.theregister.co.uk/2019/08/06/microsoft_reveals_nationstate_attacks_on_customer_IoT_devices/ (Accessed: 15 February 2020).

Anonymous (2016) Interviewed by Raichel Collis, 26 December 2016

Anstett, A. (2019) *Newly identified remote exploit exposes WhatsApp private user data.* Available at: https://www.wandera.com/whatsapp-spyware-whats-next/(Accessed: 24 March 2020).

Apple (2018) *Unauthorized modification of iOS can cause security vulnerabilities, instability, shortened battery life, and other issues*. Available at: https://support.apple.com/en-gb/HT201954 (Accessed: 4 February 2020).

Apple (2020) *Update apps or use automatic downloads*. Available at: https://support.apple.com/en-au/HT202180 (Accessed 12 January 2020).

Apple (2021) *App store improvements.* Available at: https://developer.apple.com/support/app-store-improvements/ (accessed 31 January 2021)

Appthority (2018) 'WhatsApp Messenger and Facebook Messenger most common risky apps in the enterprise finds Appthority Q2 enterprise mobile security pulse report', *Business Wire.* Available at: http://search.ebscohost.com.ezproxyderby.ac.uk/login.aspx? direct=true&db=bwh&AN=bizwire.c85663056&site=eds-live (Accessed:4 April 2020).

Arntfield, M. (2015) ‘Towards a cybervictimology: Cyberbullying, routine activities theory, and the anti-sociality of social media’, *Canadian Journal of Communication*, 40(3).

Arthur, C. (2014) *What is Google deleting under the 'right to be forgotten' - and why?* The Guardian. Available at: https://www.theguardian.com/technology/2014/jul/04/what-is-google-deleting-under-the-right-to-be-forgotten-and-why (Accessed:23 August 2018).

Arthur, R. (2016) *10 billion items of connected clothing: the internet of things just became a lot more fashionable*. Available at: http://www.forbes.com/sites/rachelarthur/2016/04/21/10-billion-items-of-connected-clothing-the-internet-of-things-just-became-a-lot-more-fashionable/#5c52fecd4d66 (Accessed: 13 February 2017).

Ashford, W. (2014) *Apple pushes security and privacy credentials after iCloud hack*. Available at: http://www.computerweekly.com/news/2240230859/Apple-pushes-security-and-privacy-credentials-after-iCloud-hack (Accessed: 8 July 2017).

Ashford, W. (2016) *Financial sector faces era of cyber mega heists*. Available at: https://www.computerweekly.com/news/450302532/Financial-sector-faces-era-of-cyber-mega-heists (Accessed: 8 August 2018).

Ashford, W. (2019) *Social media and enterprise apps pose big security risks*. Available at: https://www.computerweekly.com/news/252469873/Social-media-and-enterprise-apps-pose-big-security-risks (Accessed: 20 March 2020).

Ashok, I. (2016) *Russia's Facebook VK hacked and 100 million accounts on sale in the dark web*. Available at: http://www.ibtimes.co.uk/hackers-selling-100-million-stolen-russian-social-media-accounts-dark-web-1563805 (Accessed: 9 February 2017).

Ashton, K. (2018) 'That 'Internet of Things' thing', *RFID journal.* Available at: http://www.itrco.jp/libraries/RFIDjournal-That%20Internet%20of%20Things%20Thing.pdf (Accessed: 22 June 2020).

Ashton, K. (2019) Interviewed by Evan Davis, *The Bottom Line* , BBC Radio 4, 31 January

Asthana, A. and McVeigh, T. (2010) *Government services to be online-only.* The Guardian. Available at: https://www.theguardian.com/society/2010/nov/20/ government-services-online-only (Accessed: 21 August 2018).

Australian Cyber Security Centre (ACSC) (2019) *Software updates.* Available at: https://www.staysmartonline.gov.au/protect-yourself/protect-your-stuff/software-updates (Accessed: 28 October 2019).

Azucar, D., Marengo, D. and Settanni, M. (2018) 'Predicting the Big 5 personality traits from digital footprints on social media: A meta-analysis', *Personality and Individual Differences*, 124, pp.150-159.

Bandhakavi, S., Tiku, N., Pittman, W., King, S.T., Madhusudan, P. and Winslett, M. (2011) 'Vetting browser extensions for security vulnerabilities with VEX', *Communications of the ACM*, 54(9), p. 91. doi: 10.1145/1995376.1995398.

Bank of England (2015) *Financial stability report* [PDF] Available at http://www.bank of England.co.uk/publications/Documents/fsr/2015/fsrfull1507.PDF (Accessed: 12 December 2015)

Bank of England (2016a) *CBEST Implementation guide*. Available at: www.bankofengland.co.uk/financialstability/fsc/.../cbestimplementationguide.pd. (Accessed: 13 June 2016).

Bank of England(2016b)*CBEST intelligence-led testing version 2.0* Available at: https://www.bankofengland.co.uk/-/media/boe/files/financial-stability/financial-sector-continuity/cbest-implementation-guide.pdf (Accessed 25 October 2019).

Bank of England (2016c) *Understanding cyber threat intelligence operations* https://www.bankofengland.co.uk/-/media/boe/files/financial-stability/financial-sector-continuity/understanding-cyber-threat-intelligence-operations.pdf. (Accessed 25 October 2019).

Bank of England (2019 a) *What does the Bank of England do?* Available at: https://www.bankofengland.co.uk/about (Accessed: 12 May 2019).

Bank of England (2019 b) *What is the Prudential Regulation authority?* Available at: https://www.bankofengland.co.uk/knowledgebank/what-is-the-prudential-regulation-authority-pra (Accessed: 12 May 2019)

Bank of England (2020) *Financial sector continuity. Available at:* https://www.bankofengland.co.uk/financial-stability/financial-sector-continuity. (Accessed:6 July 2020).

Barcena, M.B. and Wueest, B.C. (2015) *Insecurity in the internet of things.* Available at https://www.symantec.com/content/en/us/entereprise/fact_sheet/b-insecurity-in-the -internet-of-things-ds.PDF (Accessed: 3 July 2016)

Bartolacci, M.R., LeBlanc, L.J., Vanderbilt, Podhradsky, A. and State, D. (2014) 'Personal denial of service (PDOS) attacks: A discussion and exploration of a new category of Cybercrime', *Journal of Digital Forensics, Security and Law*, 9(1), pp. 19–36.

Batt, S. (2019) *How malware developers target illegal streaming.* Available at: https://www.maketecheasier.com/malware-developers-target-illegal-streaming/ (Accessed 7 November 2019).

Bauman, Z. (2000) *Liquid modernity*. Oxford: Polity. Available at: http://search.ebscohost.com.ezproxy.derby.ac.uk/login.aspx?direct=true&db=cat01750a&AN=udc.928735&site=eds-live (Accessed: 23 May 2020).

BBC Bitesize (2020) *Computer Misuse Act.* Available at: https://www.bbc.co.uk/bitesize /guides/zt8qtfr/revision/1. (Accessed: 17 May 2020).

BBC News (2016) *Identity fraud up by 57% as thieves 'hunt' on social media*. Available at: https://www.bbc.co.uk/news/uk-36701297 (Accessed: 17 January 2017)

BBC News (2017) *Cyber-attack threat escalating - Europol*. Available at: https://www.bbc.co.uk/news/technology-39913630 (Accessed: 29 October 2019).

BBC News (2018) *Malicious fax leaves firms open to attack*. Available at: https://www.bbc.co.uk/news/technology-45083774 (Accessed: 23 August 2018).

BBC News (2019a) *Indians among those 'targeted' by WhatsApp spyware*. Available at: https://www.bbc.co.uk/news/world-asia-india-50245209 (Accessed: 19 November 2019).

BBC News (2019b) *New WhatsApp breach: India cyber cell urges update*. Available at: https://www.bbc.co.uk/news/world-asia-india-50470476 (Accessed: 19 November 2019).

BBC News (2020a) *One billion Android devices at risk of hacking*. Available at: https://www.bbc.co.uk/news/technology-51751950 (Accessed: 6 March 2020).

BBC News (2020b) *TV watching and online streaming surge during lockdown*. Available at: https://www.bbc.co.uk/news/entertainment-arts-53637305 (Accessed 22 June 2021).

BBC News (2021) *Pandemic accelerated UK's shift online, says Ofcom*. Available at: https://www.bbc.co.uk/news/technology-57383998 (Accessed 22 June 2021).

Beck, U. (1992) *Risk society : towards a new modernity*. Translated by Ritter, M. London: Sage

Beckstead, N., Bostrom, N., Bowerman, N., Cotton-Barratt, O., MacAskill, W., Ó hÉigeartaigh, S. and Ord, T. (2014) *Unprecedented technological risks*. Future of Humanity Institute. Available at: https://www.fhi.ox.ac.uk/wp-content/uploads /Unprecedented-Technological-Risks.PDF. (Accessed: 3 September 2018).

Behrens, S. (2009) ‘Shadow systems’, *Communications of the ACM*, 52(2), p. 124. doi: 10.1145/1461928.1461960

Bello, L. and Pistoia, M. (2018) ‘ARES : Triggering payload of evasive Android malware’, *Mobile Software Engineering and Systems*. (International Conference on Software Engineering), p.2 doi: 10.1145/3197231.3197239.

Bennett, M. (2016) *Saying goodbye to the traditional IT department.* The Telegraph. Available at: https://www.telegraph.co.uk/business/ready-and-enabled/demise-of-the-it-department/ (Accessed: 8 September 2018).

Bergman, M. K. (2001) *The deep web: Surfacing hidden value*. Available at: https://brightplanet.com/wp-content/.../03/12550176481-deepwebwhitepaper1.PDF (Accessed: 28 March 2018).

Bergman, S.M., Fearrington, M.E., Davenport, S.W. and Bergman, J.Z. (2011) ‘Millennials, narcissism, and social networking: What narcissists do on social networking sites and why’, *Personality and Individual Differences*, 50(5), pp. 706–711. doi: 10.1016/j.paid.2010.12.022.

Bertino, E. and Islam, N. (2017) ‘Botnets and Internet of things security’, *Computer*, 50(2), pp. 76–79. doi: 10.1109/mc.2017.62.

Besnard, D. and Arief, B. (2004) ‘Computer security impaired by legitimate users’, *Computers and Security*, 23(3), pp. 253–264. doi: 10.1016/j.cose.2003.09.002.

Bickford, J., O'Hare, R., Baliga, A., Ganapathy, V. and Iftode, L (2010) ‘Rootkits on smart phones: Attacks, implications and opportunities’. *HotMobile '10: Eleventh workshop on mobile computing systems and applications.* Annapolis, Maryland. February. Available at: https://www.researchgate.net/publication /234787968 _ Rootkits_on_smart_phones_Attacks_implications_and_ opportunities (Accessed: 21 June 2020).

Bishop, M. (2002) *Computer security: Art and science.* Addison Wesley Professional.

Black, M. (2020) *Most common WhatsApp scams*. Available at: https://www.techadvisor.co.uk/how-to/software/whatsapp-scams-3331146/ (Accessed 8 June 2020).

Blake, K., Bastian, B., Denson, T., Grosjean, P. and Brooks, R. (2018). *Income inequality not gender inequality positively covaries with female sexualization on social media*. PNAS published ahead of print, August 21, 2018 https://doi.org/10.1073/pnas.1717959115

Blanco, O. (2020) *How to avoid Facebook Messenger scams*. Available at: https://www.consumerreports.org/scams-fraud/facebook-messenger-scams-how-to-avoid/(Accessed: 5 April 2020).

Bode, K. (2018) *The rise of Netflix competitors has pushed consumers back toward piracy*. Available at: https://www.vice.com/en_us/article/d3q45v/bittorrent-usage-increases-netflix-streaming-sites (Accessed: 12 November 2019).

Bond, D. (2018) *Seven UK banks targeted by co-ordinated cyber-attack* | Financial Times. Available at: https://www.ft.com/content/2e582594-48ab-11e8-8ee8-cae73aab7ccb (Accessed: 23 August 2018).

Bond Dickinson Job Description (2016) Available at https://www.allhires.com/bonddickinson/PositionDetail.aspx?id=1883&a=&n=&retu rl=%2fbonddickinson%2f (Accessed: 25 November 2016)

Boricha, M. (2021) *14 Best game hacker apps for Android (With/Without Root)* Available at: https://techrrival.com/best-game-hacker-apps-android/ (Accessed 5 February 2021)

Botelho, B. (2013) *Explained: what is the Internet of Things?* Available at: http://internetofthingsagenda.techtarget.com/feature/Explained-What-is-the-Internet-of-Things (Accessed: 5 September 2016).

Brantingham, P. and Brantingham, P. (1991) Notes on the geometry of crime. In Brantingham, P. and Brantingham, P. (Eds.) *Environmental criminology*. Prospect Heights Ill, Waveland Press, pp.27–54.

Bradbury, D. (2014) 'Unveiling the dark web', *Network Security*, (4), pp. 14–17. doi: 10.1016/S1353-4858(14)70042-X.

Breakey, H. (2018) 'Deliberate, principled, self-interested law breaking: The ethics of digital 'piracy'', *Oxford Journal of Legal Studies*, 38(4), pp. 676–705.

Britton, K. (2016) 'Handling privacy and security in the internet of things', *Journal of Internet Law*, 19(10), pp. 3-7, Business Source Premier, EBSCO*host*, viewed 16 February 2017.

Broadhurst, R., Grabosky, P., Alazab, M. and Chon, S. (2014) 'Organizations and cybercrime: An analysis of the nature of groups engaged in cybercrime', *International Journal of Cyber Criminology,* **8**(1), pp. 1-20.

Brown, N. (2015) 'Epistemology', *Social research and practice and education Ltd*, 3 November. Available at: http://www.nicole-brown.co.uk/epistemology/ (Accessed: 23 June 2020).

Brown, T. (2016) ‘Future of Work’ *Raconteur independent publication* 0421.

Bryman, A.(2012) *Social research methods*. 4th edn, Oxford: Oxford University Press

BT (2018) *What is a smart plug? Connect your home appliances through the magic of Wi-Fi*. Available at: http://home.bt.com/tech-gadgets/internet/connected-home/what-is-a-smart-plug-connect-your-home-appliances-through-the-magic-of-wi-fi-11364278610761 (Accessed: 11 February 2020).

Bucher, B.(2020) *Messaging app usage statistics around the world*. Available at: https://www.messengerpeople.com/global-messenger-usage-statistics/ (Accessed: 24 March 2020).

Burles, M. C. and Bally, J. M. G. (2018) ‘Ethical, practical, and methodological considerations for unobtrusive qualitative research about personal narratives shared on the internet’, *International Journal of Qualitative Methods*, 17(1), pp. 1–9. doi: 10.1177/1609406918788203.

Burns, A.J., Johnson, M.E. and Caputo, D.D. (2019) ‘Spear phishing in a barrel: Insights from a targeted phishing campaign’, *Journal of Organizational Computing and Electronic Commerce*, 29(1), pp.24–39.

Business Dictionary (2019) *Professional Bodies*. Available at: http://www.businessdictionary.com/definition/professional-body.html. (Accessed: 13 May 2019).

Byrne, Z.S., Dvorak, K.J., Peters, J.M., Ray, I., Howe, A. and Sanchez, D. (2016) ‘From the user’s perspective: Perceptions of risk relative to benefit associated with

using the Internet', *Computers in Human Behavior*, 59, pp. 456–468. doi: 10.1016/j.chb.2016.02.024

Caballero, J., Grier, C., Kreibich, C. and Paxson, V. (2011) Measuring pay-per-install: The commoditization of malware distribution. *IMDEA Software Institute.* Available at: https://software.imdea.org/~juanca/papers/ppi_usenixsec11.pd (Accessed: 30 August 2018).

Cabinet Office (2016) *The UK cyber security strategy annual report 2011 - 2016*. Available at: https://www.gov.uk/.../UK_Cyber_Security_Strategy_Annual_ Report_2016.PDF (Accessed: 13 June 2016).

Capeller, W. (2001) 'Not such a neat net: Some comments on virtual criminality', *Social and Legal Studies*, 10(2), pp.229-242.

Carpenter, C.J. (2012) 'Narcissism on Facebook: Self-promotional and anti-social behaviour', *Personality and Individual Differences*, 52(4), pp. 482–486. doi: 10.1016/j.paid.2011.11.011.

Carr, M. (2019) Interviewed by Evan Davis, *PM,* BBC Radio 4, 3 January

Carrino, F., Mugellini, E., Abou Khaled, O., Ouerhani, N. and Ehrensberger, J. (2016) 'INUIT: Internet of Things for urban innovation', *Future Internet*, 8(2), p. 18. doi: 10.3390/fi8020018.

Carter, J. (2015) *What is the 'shadow' Internet of Things – and how dangerous is it?* Available at: http://www.techradar.com/news/internet/what-is-the-shadow-internet-of-things-and-how-dangerous-is-it--1300288 (Accessed: 18 December 2015).

Castells, M. (2001) *The internet galaxy. Reflections on the internet, business and society*. Oxford: Oxford University Press

Castells, M. (2005) The network society: From knowledge to policy. In Castells, M. and Cardoso, G. Eds. 2005, *The network society: From knowledge to policy.* Washington, DC: Johns Hopkins Centre for Transatlantic Relations, pp 3-21

Castells, M. (2011) 'A network theory of power', *International Journal of Communication* 5 pp 773-787. Available at: http://ijoc.org/index.php/ijoc/article/view/1136/553. Accessed: 31 August 2018).

Chaffey, D. (2020) *Video marketing statistics to know for 2020*. Available at: www.smartinsights.com/digital-marketing-platforms/video-marketing/video-marketing-statistics-to-know/(Accessed: 7 July 2020).

Chan, A. (2017) *How the internet of things is the perfect target for DDoS attacks and data breaches*. Available at: http://www.techtimes.com /articles /191478/20170114 /how-internet-of-things-devices-are-the-perfect-target-for-ddos-attacks-and-data-breaches.htm (Accessed: 6 February 2017).

Chapman, N. (2015) *The dark shadow cast by the IoT: the potential for security nightmares.* Available at: https://www.techradar.com/uk/news/world-of-tech/the-dark-shadow-cast-by-the-iot-the-potential-for-security-nightmares-1285791(Accessed: 25 January 2017).

Charara, S. (2017) *Semi-precious: The best smart jewellery*. Available at: https://www.wareable.com/smart-jewellery/semi-precious-the-best-smart-jewelry-582 (Accessed: 13 February 2017).

Chaudhry, P.E. (2017a) ‘The looming shadow of illicit trade on the internet’, *Business Horizons*, doi: 10.1016/j.bushor.2016.09.002.

Chaudhry, S. (2017b) ‘What does a ‘cracked PC game’ mean?’ *Quora,* 22 April. Available at: https://www.quora.com/What-does-a-%E2%80%98cracked-PC-game%E2%80%99-mean/answer/Shahmeer-Chaudhry. Accessed July 2020

Checkland, P. and Poulter, J. (2007) *Learning for action: A short definitive account of soft systems methodology, and its use for practitioners, teachers and students.* Chichester: John Wiley.

Checkpoint (2019) *Cyber-attack trends: mid-year report***.** Available at: https://research.checkpoint.com/2019/cyber-attack-trends-2019-mid-year-report/ (Accessed 12 June 2020).

Chen, P.S., Lin, S.-C. and Sun, C.-H. (2015) ‘Simple and effective method for detecting abnormal internet behaviours of mobile devices’, *Information Sciences*, 321, pp. 193–204. doi: 10.1016/j.ins.2015.04.035.

Cheong, Y., Jensen, A., Gudnadottir, E., Bae, B. and Togelius, J. (2015) ‘Detecting predatory behavior in game chats’, *IEEE Transactions on Computational Intelligence and AI in Games*, 7(3), pp.220-232.

Cherowbrier, J. (2020)*Total financial services employment 2019.* Available at: https://www.statista.com/statistics/298370/uk-financial-sector-total-financial-services-employment/ (Accessed: 4 May 2020).

Chik, W.B. (2007) ‘Challenges to criminal law making in the new global information society: A critical comparative study of the adequacies of computer-

related criminal legislation in the United States, the United Kingdom and Singapore in *Cybercrime and the Law.* Icfai Law Books.

Christensen, B. (2003) *What is a Facebook survey scam?* Available at: http://www.hoax-slayer.com/what-is-a-survey-scam.shtml (Accessed: 9 February 2017).

Childline (2018) *Taking care of your digital footprint.* Available at: https://www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/taking-care-your-digital-footprint/. (Accessed: 23 August 2018).

Choi, S., Martins, J.T. and Bernik, I. (2018) Information security: Listening to the perspective of organisational insiders. *Journal of information science*, 44(6), pp.752–767.

Cimpanu, C. (2019a) *Mysterious hacker has been selling Windows 0-days to APT groups for three years*. Available at: https://www.zdnet.com/article/mysterious-hacker-has-been-selling-windows-0-days-to-apt-groups-for-three-years/ (Accessed 9 Jun. 2020).

Cimpanu, C. (2019b) *New 'unremovable' xHelper malware has infected 45,000 Android devices. Factory resets aren't helping. Neither are mobile antivirus solutions. Malware keeps reinstalling itself.* Available at: https://www.zdnet.com/article/new-unremovable-xhelper-malware-has-infected-45000-android-devices/ (Accessed 25 June 2020).

Cimpanu, C. (2019c) *Android bug lets hackers plant malware via NFC beaming .* Available at: https://www.zdnet.com/article/android-bug-lets-hackers-plant-malware-via-nfc-beaming/ (Accessed: 19 November 2019).

Cimpanu, C. (2019d) *FBI recommends that you keep your IoT devices on a separate network.* Available at: https://www.zdnet.com/article/fbi-recommends-that-you-keep-your-IoT-devices-on-a-separate-network/ (Accessed:20 February 2020).

CisoMag (2020) *WhatsApp bug allowed hackers to steal files and messages with gifs*. Available at: https://www.cisomag.com/a-malicious-gif-image-sent-via-whatsapp-could-hack-your-android-phone/ (Accessed: 5 April 2020).

Clarke, S. (2016) 'Reducing the impact of cyberthreats with robust data governance', *Computer Fraud and Security*, 2016(7), pp. 12–15. doi: 10.1016/s1361-3723(16)30053-7.

Clement, J. (2019a) *Mobile payments worldwide - Statistics and Facts* https://www.statista.com/topics/4872/mobile-payments-worldwide/

Clement, J. (2019b) *Mobile apps that have been used only once 2019.* Available at: https://www.statista.com/statistics/271628/percentage-of-apps-used-once-in-the-us/ (Accessed: 21 December 2019).

Clement, J. (2020a) *Global digital population 2019* Available at: https://www.statista.com/statistics/617136/digital-population-worldwide/ (Accessed 6 May 2020).

Clement, J. (2020b) *Share of global mobile website traffic 2015-2020* Available at:https://www.statista.com/statistics/277125/share-of-website-traffic-coming-from-mobile-devices/ (Accessed: 21 June 2020).

Clement, J. (2020c) *Device usage of Facebook users worldwide as of April 2020* Available at: https://www.statista.com/statistics/377808/distribution-of-facebook-users-by-device/(Accessed 21 June 2020).

Clement, J. (2020d) *Global Snapchat user distribution by gender 2020*. Available at: https://www.statista.com/statistics/326460/snapchat-global-gender-group/ (Accessed: 6 April 2020).

Cloudflare (2020) *What is a malicious payload?* Available at: https://www.cloudflare. com/learning/security/glossary/malicious-payload/ (Accessed: 11 June 2020)

Cohen, L.E. and Felson, M. (1979) 'Social change and crime rate trends: A routine activity approach', *American Sociological Review*, 44(4), p. 588.-608 doi: 10.2307/2094589.

Coles, R. and Hodgkinson, G. (2008) 'A psychometric study of information technology risks in the workplace', *Risk Analysis: An International Journal*, 28, 1, pp. 81-93, Business Source Premier, EBSCO*host*, viewed 25 August 2016.

Colwill, C. (2009) 'Human factors in information security: The insider threat – who can you trust these days?', *Information Security Technical Report*, 14(4), pp. 186–196. doi: 10.1016/j.istr.2010.04.004.

Constine, J. (2017) *Instagram's growth speeds up as it 'hits' 700 million users*. Available at: https://techcrunch.com/2017/04/26/instagram-700-million-users (Accessed: 2 August 2017).

Cook, S. (2019) The *complete list of streaming services - 100+ services.* Available at: https://flixed.io/complete-list-streaming-services/ (Accessed: 31 October 2019).

COP Guidance (2013) *Research guidance note 4 online survey tools*. Available at: http://staff.napier.ac.uk/services/research-innovation-office/policies/Documents/Integrity/COPguidance4.PDF (Accessed: 17 May 2016).

Coorevits, L. and Coenen, T. (2016) 'The rise and fall of wearable fitness trackers', *Academy of Management Annual Meeting Proceedings*, (1), pp.1-24 Available at: https://biblio.ugent.be/publication/8055995/file/8510819.pdf (Accessed 23June 2020).

Corbyn, Z. (2019). *Are brain implants the future of thinking?* https://www.theguardian.com/science/2019/sep/22/brain-computer-interface-implants-neuralink-braingate-elon-musk (Accessed 24 May 2020).

Corman, J. (2013) *Swimming with sharks - security in the internet of things* TEDx Talk, Naperville. Available at http://tedxtalks.ted.com/video.mason/Swimming-with-sharks-security (Accessed: 20 September 2016)

Costin, A. and Zaddach, J.(2018) *IoT malware: comprehensive survey, analysis framework and case studies.* Available at: https://www.semanticscholar.org/paper/IoT-Malware-%3A-Comprehensive-Survey-%2C-Analysis-and-Costin/8ce50a54cec57c71f8f01ecb29bc086bee14bc91 (Accessed: 9 April 2020).

Coulson, N. (2015) *Online research methods for psychologists*. United Kingdom: Palgrave Macmillan.

Coward, J. (2018) *Funny IoT devices: Is this the worst of the internet of things?* Available at: https://www.IoTworldtoday.com/2018/02/19/funny-IoT-devices-worst-internet-things/.(Accessed: 22 June 2020)

Crane, C. (2020) 'The Definitive Cyber Security Statistics Guide for 2020', *The SSL Store,* May 14. Available at: https://www.thesslstore.com/blog/cyber-security-statistics/#insider-threats-intentional-or-negligence (Accessed 10 June 2020).

Crookes, A. (2016) 'Readers Comments', *Gadgets',* 08 January. Available at https://gadgets.ndtv.com/apps/features/how-to-turn-off-automatic-app-updates-in-android-ios-windows-phone-81-windows-81-634685. (Accessed: 28 October 2019).

Cross ,N. (1982) 'Designerly ways of knowing' *Design Studies',*3 (4) pp 221-227.

Cross, N. (2001) 'Designerly ways of knowing: Design discipline versus design science', *Design Issues*. 17(3):49-55.

Crossler, R., Johnston, A., Benjamin Lowry, P., Hu, Q., Warkentin, M. and Baskerville, R. (2013) 'Future directions for behavioural information security research', *Computers and Security*, 32, pp.90 -101.

Cullen, C. (2018) 'Global Internet Phenomena Preview: File Sharing on The Internet Reverses A Downward Trend', *Sandvine,* 24 September. Available at: https://www.sandvine.com/blog/global-internet-phenomena-preview-file-sharing-reverses-a-downward-trend (Accessed: 12 November 2019).

Cuthbertson, A. (2019a) *Game of Thrones stream sites that let fans watch Season 8 online for free benefit from 'piracy mania'*. Available at: https://www.independent.co.uk/life-style/gadgets-and-tech/news/game-of-thrones-season-8-episode-2-stream-download-torrent-piracy-a8876691.html (Accessed: 12 November 2019).

Cuthbertson, A. (2019b) *WhatsApp bug let hackers read your messages with a video*. Available at: https://www.independent.co.uk/life-style/gadgets-and-tech/news/whatsapp-bug-messages-hack-android-update-ios-mp4-video-a9206901.html (Accessed: 24 March 2020).

Daly, R. (2016) *There's no place like phone consumer usage patterns in the era of peak smartphone*. Available at: http://www.deloitte.co.uk/mobileuk/assets/PDF/Deloitte-Mobile-Consumer-2016-There-is-no-place-like-phone.PDF (Accessed: 4 October 2016).

Danezis, G., Domingo-Ferrer, J., Hansen, M., Hoepman, J.H., Le Métayer, D., Tirtea, R. and Schiffner, S. (2014) *Privacy and data protection by design – from policy to engineering*. Available at: https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design (Accessed: 24 June 2021).

Darabian, H., Dehghantanha, A., Hashemi, S., Homayoun, S. and Choo, K.R. (2020) 'An opcode-based technique for polymorphic Internet of Things malware detection', *Concurrency and Computation: Practice and Experience*, 32(6)

Darafsheh, S. (2019) *IoT applications in eyewear.* Available at: https://www.IoTforall.com/IoT-applications-eyewear/ (Accessed: 9 May 2020).

Daryabar, F., Dehghantanha, A., Eterovic-Soric, B. and Choo, K.K.R. (2015) ‘Forensic investigation of OneDrive, Box, GoogleDrive and Dropbox applications on Android and iOS devices’, *Australian Journal of Forensic Sciences*, 48(6), pp. 615–642. doi: 10.1080/00450618.2015.1110620.

Das, S. and White, G. (2019) **‘**Instagram sends predators to accounts of children as young as 11’ *The Sunday Times,* 1 December.

Dassanayake, D. (2019) *Instagram and Snapchat warning - alert about this scary scam, do not fall for it*. Available at: https://www.express.co.uk/life-style/science-technology/1116140/Instagram-and-Snapchat-warning-scam-alert-April-19 (Accessed: 6 April 2020).

Davies, C. and Fisher, M. (2018) ‘Understanding research paradigms’, *Journal of the Australasian Rehabilitation Nurses’ Association (JARNA)*, 21(3), pp. 21–25. Available at: https://search-ebscohost-com.ezproxy.derby.ac.uk/login. aspx?direct =true&db =ccm&AN=134014168& site=eds-live (Accessed: 10 July 2020).

Davies, M., Read, H., Xynos, K. and Sutherland, I. (2015) ‘Forensic analysis of a Sony PlayStation 4: A first look’, *Digital Investigation*, 12, pp. 81-89.

Davis, G. (2018) **‘**What to Do When Your Social Media Account Gets Hacked, *McAfee,* 3 December. Available at: https://www.mcafee.com/blogs/consumer/ consumer-threat-notices/social-media-account-hacked/ (Accessed: 23 May 2020).

Davis, J. L. (2014) ‘Triangulating the self: Identity processes in a connected era’, *Symbolic Interaction,* 37 (4) pp. 500-523

Deloitte (2019) *Global mobile consumer survey: UK cut. Plateauing at the peak; the state of the smartphone*. Available at: https://www2.deloitte.com/uk/en

/pages/technology-media-and-telecommunications/articles/mobile-consumer.html (Accessed: 17 March 2020).

DeNisco Rayome, A. (2018) *Smart plug flaw gives hackers access to business networks, highlights IoT security challenges*. Available at: https://www.techrepublic.com/article/smart-plug-flaw-gives-hackers-access-to-business-networks-highlights-IoT-security-challenges/ (Accessed: 11 February 2020).

Dennis (2018) *How cookies track you around the web and how to stop them.* Available at: https://privacy.net/stop-cookies-tracking/ (Accessed: 18 September 2018).

Deschamps-Sonsino, A. (2017) Interviewed by Aleks Krotoski for BBC Radio 4 *Aleks in Wonderland*, 30 August. Available at http://www.bbc.co.uk/programmes/b092fszv (Accessed: 29 November 2017).

Dharmavaram, V.G. (2015) 'Clickjacking: A study on popular websites in India', *Journal of Money Laundering Control*, 18(4), pp. 447–456. doi: 10.1108/jmlc-11-2014-0046.

Digital Shadows (2015) *CBEST/STAR threat intelligence.* Available at: https://www.digitalshadows.com/assets/Uploads/cbest/DS-CBEST-STAR-Overview.pdf. (Accessed: 23 July 2020).

Dodge, N. and Chapman, R. (2018) 'Investigating recruitment and completion mode biases in online and door to door electronic surveys', *International Journal of Social Research Methodology*, 21 (2) pp. 149-163.

Doffman, Z. (2019) *New Android threat: Google confirms malicious apps removed from play store—uninstall now.* Available at: https://www.forbes.com/sites/zakdoffman /2019/11/06/new-google-android-threat-these-7-malicious-apps-may-be-downloading-malware-onto-your-phone/#3e84c57375af (Accessed 6 May 2020).

Dohr, A., Modre-Opsrian, R., Drobics, M., Hayn, D. and Schreier, G. (2010) 'The Internet of Things for ambient assisted living', *2010 Seventh International Conference on Information Technology: New Generations*, doi: 10.1109/itng.2010.104.

Domingo-Ferrer, J. and Blanco-Justicia, A. (2020) Privacy-preserving technologies. In: Christen, M., Gordijn, B. and Loi, M. (eds) *The ethics of cybersecurity*. The International Library of Ethics, Law and Technology, vol 21. CHAM. https://doi.org/10.1007/978-3-030-29053-5_14. Available at: https://link.springer.com/chapter/10.1007/978-3-030-29053-5_14 (Accessed: 24 June 2021).

Domo (2017) *Data never sleeps 5.0.* Available at: https://www.domo.com /learn/data-never-sleeps-5 (Accessed: 11 December 2017).

Donovan, J. (2016) '"Can you hear me now?" Phreaking the party line from operators to occupy', *Information, Communication and Society*, 19(5), pp. 601–617. doi: 10.1080/1369118x.2016.1139610.

Doshi, N., Athalye, A. and Chien, E. (2010) *Pay-per-install. The new malware distribution network*. Available at: https://www.symantec.com/content

/dam/symantec/docs/security-center/white-papers/security-response-pay-per-install-10-en.PDF.(Accessed: 30 August 2018).

Dredge, S. (2014) *Coding at school: a parent's guide to England's new computing curriculum*. Available at: https://www.theguardian.com/technology/2014/sep /04/coding-school-computing-children-programming (Accessed: 29 October 2018).

Drew, J., Hahsler, M. and Moore, T.(2017) 'Polymorphic malware detection using sequence classification methods and ensembles', *EURASIP Journal on Information Security* **2017,** 2 doi.org/10.1186/s13635-017-0055-6

Dubach, I. (2018) *New study reveals why women take sexy selfies.* Available at: https://phys.org/news/2018-08-reveals-women-sexy-selfies.html (Accessed: 15 September 2018).

Dungay, D. (2019) *Instant messaging apps put financial institutions at risk* Available at: https://www.commsbusiness.co.uk/news/instant-messaging-apps-put-financial-institutions-at-risk/(Accessed: 6 April 2020).

Eadicicco, L. (2020) *Elon Musk says there's a chance his AI-brain-chip company will be putting implants in humans within a year*. Available at: https://www.businessinsider.com/elon-musk-neuralink-brain-chip-put-in-human-within-year-2020-5?r=US IR=T (Accessed 24 May 2020).

Eddy, M. (2020) *The best VPN services for 2020.* Available at: https://uk.pcmag.com/vpn/138/the-best-vpn-services (Accessed: 23 July 2020).

Ellis, L., Saret, J.S. and Weed, P. (2012) 'BYOD: From company-issued to employee-owned devices', *Telecom, Media and High-Tech Extranet, (No. 20*

Recall.PDF) Available at: http:// www.mckinsey.com (Accessed: 11 January 2016).

Emm, D. (2020) *IT threat evolution Q1 2020*. Available at: https://securelist.com/it-threat-evolution-q1-2020/96886/, (Accessed 19 June 2020).

ENISA European Union Agency for Cybersecurity (2012) *Botnets: measurement, detection, disinfection and defence*. Available at: https://www.enisa.europa.eu /publications/botnets-measurement-detection-disinfection-and-defence (Accessed: 9 February 2017).

ENISA European Union Agency for Cybersecurity (2017) *Supply chain attacks*. Available from: https://www.enisa.europa.eu/publications/info-notes/supply-chain-attacks (Accessed: 17 September 2019).

Ernst and Young Global Ltd (2015) *Cybersecurity and the Internet of Things insights on governance, risk and compliance*. Available at: http://www.ey.com/Publication/ vwLUAssets/EY-cybersecurity-and-the-internet-of-things/$FILE/EY-cybersecurity-and-the-internet-of-things.PDF (Accessed: 18 December 2015).

Esposito, J. (2017) 'Malware spread through Pornhub', *Kaspersky,* 10 October. Available at: https://www.kaspersky.com/blog/pornhub-malvertising/19698/ (Accessed: 19 March 2020).

EUIPO, European Union Intellectual Property Office (2018) I*dentification and analysis of malware on selected suspected copyright- infringing websites.* Report. pp.12 -13. Available at: https://euipo.europa.eu/tunnel-web/secure/webdav/

guest/document_library/observatory/documents/reports/ /2018_Malware_ Study_en.PDF (Accessed: 7 November 2019).

Evans, P. (2019) ‘Melody VR app puts music festival fans in the front row’, *The Sunday Times* , 21 July.

Eysenbach, G. and Till, J. E. (2001) ‘Ethical issues in qualitative research on internet communities’, *BMJ (Clinical research ed.)*, 323(7321), pp. 1103–1105. Available at: http://search.ebscohost.com.ezproxy.derby.ac.uk/login.aspx?direct=true&db=cmedm&AN=11701577&site=eds-live (Accessed: 27 June 2020).

Facebook (2018) *What is tagging and how does it work?* Facebook Help Centre (Accessed: 18 September 2018).

Fact (2017) C*racking down on digital piracy*. Available at: https://www.fact-uk.org.uk/files/2017/09/Cracking-Down-on-Digital-Piracy-Report-Sept-2017.PDF. (Accessed: 7 November 2019).

Fan, X. (2015) ‘Tracking and taxonomy of cyberlocker link sharers based on Behavior Analysis’, *The Journal of Digital Forensics, Security and Law*, 10(4).

FBI (2014) *GameOver Zeus botnet disrupted*. Available at: https://www.fbi.gov /news/stories/gameover-zeus-botnet-disrupted (Accessed: 7 February 2017).

Fehér, K. (2017) ‘Net framework and the digitalized mediatized self’, *Corvinus Journal of Sociology and Social Policy*, 8(1), pp.111-126.

Field, M. and Murphy, M. (2018) *Strava fitness app divulges heatmap of secretive British SAS base.* Available at: https://www.telegraph.co.uk/technology

/2018/01/29 /strava-fitness-app-divulges-heatmap-secretive-british-sas-base/(Accessed: 19 May 2020).

Fielding, J. (2020) ‘The people problem: how cyber security's weakest link can become a formidable asset, *Computer Fraud and Security*,(1), pp. 6–9.

Financial Conduct Authority (2016) *About the FCA*. Available at: https://www.fca.org.uk/about/the-fca (Accessed: 12 May 2019).

Financial Services Compensations Scheme (2019) Available at http://fscsjobs.org.uk / (Accessed: 12 May 2019).

Fireeye (2019) *Email threat report Q1.* Available at: https://content.fireeye.com /one-email/rpt-email-threat-report-2019-Q1-en (Accessed 10 June 2020).

Fitbit (2018) *Make payments easy with Fitbit Pay.* Available at: https://www.fitbit.com/fitbit-pay (Accessed: 2 September 2018).

Fisher, P. (2015) ‘CBEST Demystified E-book’ *Nettitude,* 19 May. Available at: https://blog.nettitude.com/uk/nettitude-releases-new-ebook-cbest-demystified (Accessed: 22 July 2020).

Foddy, W. (2011) *Constructing questions for interviews and questionnaires*. Cambridge, Cambridge University Press.

Forrest, C. (2016) *The state of mobile device security: Android vs. IOS*. Available at: http://www.zdnet.com/article/the-state-of-mobile-device-security-android-vs-ios/ (Accessed: 6 February 2017).

Forsgren, E. and Byström, K. (2018) ‘Multiple social media in the workplace: Contradictions and congruencies’, *Information Systems Journal*, 28(3), pp. 442–464. doi: 10.1111/isj.12156.

Francis, B. (2018) ‘How to Build Your Own Private Smart Home with A Raspberry Pi and Mozilla’s Things Gateway’ *Mozilla Hacks - the Web Developer Blog,* 6 February. Available at: https://hacks.mozilla.org/2018/02/how-to-build-your-own-private-smart-home-with-a-raspberry-pi-and-mozillas-things-gateway/ (Accessed: 22 February 2020).

Frances, J., Smitheram, M., Cleveland, D,. Stephen, C. and Fisher, H. (2017) ‘Digital materiality, embodied practices and fashionable interactions in the design of soft wearable technologies’, *International Journal of Design*, 11(3), pp. 7–15.

Franklin, E. (2018) *6 ways to delete yourself from the internet*. Available at: https://www.cnet.com/how-to/remove-delete-yourself-from-the-internet/ (Accessed: 23 August 2018).

Freberg, K., Graham, K., McGaughey, K. and Freberg, L. (2011) ‘Who are the social media influencers? A study of public perceptions of personality’, *Fuel and Energy Abstracts*, 37.pp. 90-92. 10.1016/j.pubrev.2010.11.001.

Frei, S. (2014) *The known unknowns: empirical analysis of publicly unknown security vulnerabilities*. Available at: https://dev.nsslabs.com/sites/default /files/public-report/files/The%20Known%20Unknowns_1.PDF (Accessed: 7 December 2016).

Froehlich, A.F. (2015) *Shadow IT: 8 ways to cope*. Available at: http://www.informationweek.com/strategic-cio/it-strategy/shadow-it-8-ways-to-cope/d/d-id/1319535 (Accessed: 2 December 2015).

F-Secure (2019) *Attack landscape H1 2019*. Available at: https://f-secure.com/attack-landscape-h1-2019-IoT-smb-traffic-abound/ (Accessed: 15 February 2020).

Furnell, S. and Clarke, N. (2012) 'Power to the people? The evolving recognition of human aspects of security', *Computers and Security*, 31(8), pp. 983–988. doi: 10.1016/j.cose.2012.08.004.

Fürstenau, D., Rothe, H. and Sandner, M. (2020) 'Leaving the shadow: A configu rational approach to explain post-identification outcomes of shadow IT systems', *Business and Information Systems Engineering*.doi:10.1007/s12599-020-00635-2.

Gadgets 360 (2017) *How to turn off automatic app updates on Android, iPhone, iPad*. Available at: https://gadgets.ndtv.com/apps/features/how-to-turn-off-automatic-app-updates-in-android-ios-windows-phone-81-windows-81-634685 (Accessed: 28 Oct. 2019).

Galloni, A. J. (2018) *Turning social into intelligence*. Available at: https://www.professionalsecurity.co.uk/news/interviews/turning-social-into-intelligence/ (Accessed: 20 September 2018).

Garrett, M.G. (2012) 'From 'solid modernity' to 'liquid modernity'? Zygmunt Bauman and social work', *The British Journal of Social Work*, Volume 42, Issue 4, pp. 634–651, https://doi-org.ezproxy.derby.ac.uk/10.1093/bjsw/bcr094

GCF Global (2019) *Computer basics: Understanding applications*. Available at: https://edu.gcfglobal.org/en/computerbasics/understanding-applications/1/ (Accessed: 1 November 2019).

Geier, E. (2011) *Hiring hackers and buying malware is easy*. Available at: https://www.esecurityplanet.com/hackers/hiring-hackers-and-buying-malware-is-easy.html (Accessed: 30 August 2018).

Ghafur, S., Kristensen, S., Honeyford, K., Martin, G., Darzi, A. and Aylin, P. (2019) 'A retrospective impact analysis of the WannaCry cyberattack on the NHS', *NPI Digital Medicine*, 2(1), pp.1-6.

Giannoulis, P., Potamianos, G. and Maragos, P. (2019) 'Room-localized speech activity detection in multi-microphone smart homes', *EURASIP Journal on Audio, Speech, and Music Processing*, (1).

Gibbs, S. (2016) *Dropbox hack leads to leaking of 68m user passwords on the internet.* Available at: https://www.theguardian.com/technology /2016/aug/ 31/dropbox-hack-passwords-68m-data-breach (Accessed: 8 February 2017).

Gibson, S. (2004) 'Open source intelligence', *The RUSI Journal*, 149(1), pp.16-22.

Gil, P. (2016) *The best Cyberlockers*. Available at: https://www.lifewire.com/best-cyberlockers-2483584 (Accessed: 31 January 2017).

Gil González, E. and de Hert, P. (2019) 'Understanding the legal provisions that allow processing and profiling of personal data—an analysis of GDPR provisions and principles'. *ERA Forum*, 19(4), pp.597–621.

Gilligan, A. (2017) *Bosses track you night and day with wearable gadgets*. Available at: http://www.thetimes.co.uk/article/bosses-track-you-night-and-day-with-wearable-gadgets-kdn8068ql (Accessed: 13 February 2017).

Glancy, J. (2020) 'American culture increasingly dominates our digital lives. No wonder its problems feel so close to home'. *The Sunday Times Magazine* (14 June) p.7

Gokey, M. (2016) *The best smart jewellery you can buy*. Available at: http://www.digitaltrends.com/wearables/best-smart-jewelry/ (Accessed: 13 February 2017).

Goodin, D. (2019) *Armed with iOS 0days, hackers indiscriminately infected iPhones for two years*. Available at: https://arstechnica.com/information-technology/2019/08/armed-with-ios-0days-hackers-indiscriminately-infected-iphones-for-two-years/ (Accessed 6 May 2020).

Goodson, L. and Phillimore, J. (2004) 'The inquiry paradigm in qualitative tourism research' in Goodson, L. and Phillimore, J. (eds) *Qualitative research in tourism: ontologies, epistemologies and methodologies*. Taylor and Francis Group.

Goodwin, T.(2016) *The three ages of digital.* Available at: https://techcrunch. com /2016/06/23/the-three-ages-of-digital/ (Accessed: 20 June 2020)

Golubev, S. (2019) 'A Malicious Website Can Infect My iPhone. Fact or fiction?' *Kaspersky,* 4 September. Available at: https://www.kaspersky.co.uk/blog/ malicious-websites-infect-iphones/16646/ (Accessed 6 May 2020).

Google (2018) *Reasons for denial of information removal - Search Console Help*. Available at: https://support.google.com/webmasters/answer/63756 (Accessed: 23 August 2018).

Google (2020) *Remove information from Google - Google Search Help*. Available at: https://support.google.com/websearch/troubleshooter/3111061?hl=en (Accessed: 20 May 2020).

Gottfried, J. and Dost, M. (2015) *Most Millennials resist the 'Millennial' label. Generations in a mirror: How they see themselves*. Available at: http://www.people-press.org/files/2015/09/09-03-2015-Generations-release.PDF (Accessed: 25 November 2016).

GOV.UK (2016) *National cyber security strategy 2016 to 2021.* Available at: https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021 (Accessed: 26 July 2018).

GOV.UK (2019) *Plans announced to introduce new laws for internet connected devices*. Available at: https://www.gov.uk/government/news/plans-announced-to-introduce-new-laws-for-internet-connected-devices (Accessed: 17 February 2020).

Government Digital Inclusion Strategy (2014) Available at: https://www.gov.uk/government/publications/government-digital-inclusion-strategy/government-digital-inclusion-strategy (Accessed: 25 November 2016).

Grabosky, P. (2001) 'Virtual criminality: Old wine in new bottles?', *Social and Legal Studies*, 10(2), pp.243-249.

Graham, C. (2017) *NHS cyber-attack: Everything you need to know about 'biggest ransomware' offensive in history*. Available at: https://www.telegraph.co.uk/news 2017/05/13/nhs-cyber-attack-everything-need-know-biggest-ransomware-offensive/ (Accessed: 23 August 2018).

Greene, T. (2013) *Microsoft patch Tuesday targets multitude of Internet explorer faults*. Available at: http://www.networkworld.com/article/2166144/windows /microsoft-patch-tuesday-targets-multitude-of-internet-explorer-faults.html (Accessed: 26 January 2017).

Griffin, T. & Stitt, B.G. (2009) 'Random Activities Theory: The case for 'Black Swan' criminology', *Critical Criminology*. 18 (1) pp. 57-72

Grimes, R. (2017) *12 signs you've been hacked -- and how to fight back*. Available at: https://www.csoonline.com/article/2457873/data-protection/signs-youve-been-hacked-and-how-to-fight-back.html (Accessed: 4 September 2018).

GroBauer, B., Walloschek, T. and Stöcker, E. (2011) *Understanding cloud computing vulnerabilities*. Available at: http://cloudcomputing.ieee.org/images /files/publications/articles/CC_Vulnerabilities.PDF (Accessed: 04 February 2017)

Grupé,J. (2019) 'Can We Enable Wi-Fi And Mobile Data Both At The Same Time On An Android Device And Communicate Simultaneously?' *Quora* (2019) 20 June. Available at: https://www.quora.com (Accessed: 21 February 2020).

Grustniy, L.(2018) 'Mobile Malware Masked as Porn Apps*' Kaspersky,* 8 February. Available at: https://www.kaspersky.com/blog/porn-related-android-threats/21087/(Accessed: 19 March 2020).

Guay, M. (2018) ‘The 25 Best Productivity Apps’, *Zapier*, 20 September. Available at: https://zapier.com/blog/best-productivity-apps/(Accessed: 30 March 2020).

Guerra, D. (2015) *"Dead apps".* Available at: https://www.scmagazine.com/home/ opinions /dead-apps/ (Accessed: 28 January 2020).

Gulenko, I. (2013) ‘Social against social engineering’, *Information Management and Computer Security*, 21(2), pp. 91–101. doi: 10.1108/imcs-09-2012-0053.

Gupta, D. and Rani, R. (2018) Big data framework for zero-day malware detection, *Cybernetics and Systems*, 49(2), pp.103–121.

Guruswamy, K. (2016) *5 ways malware can creep into your system.* Available at: https://www.esecurityplanet.com/network-security/5-ways-malware-can-creep-into-your-system.html (Accessed:19 March 2020).

György, A.A.B., Cleven, A., Uebernickel, F. and Brenner, W. (2012) ‘Exploring the shadows: IT governance approaches to user-driven innovation’, Available at: https://www.alexandria.unisg.ch/publications/214625 (Accessed: 23 November 2016).

Hadnagy, C. (2010) *Social engineering: The art of human hacking*. Indianapolis, IN: Wiley.

Hall, C. and Zarro, M. (2012) ‘Social curation on the website Pinterest.com’, *Proceedings of the American Society for Information Science and Technology*, 49(1), pp.1-9.

Hamilton, I. A. (2019)*TikTok hit 1.5 billion downloads and is still outperforming Instagram*. Available at: https://www.businessinsider.com/tiktok-hits-15-billion-

downloads-outperforming-instagram-2019-11?r=US&IR=T (Accessed: 6 January. 2020).

Hanson, M. (2017) *Huge cyberattack leaves computers across the world reeling*, Available at: https://www.techradar.com/news/nhs-hospitals-in-england-hit-by-massive-cyberattack (Accessed: 29 October 2019).

Harari, Y.N. (2017) *Homo Deus.* Available at http://www.amazon.co.uk kindle store (Downloaded: 17 July 2017).

Hardy, E. (2018) *Estate agents add to high street malaise as firms pushed to the brink.* Available at: http://www.thisismoney.co.uk/money/markets/article-6071159/Estate-agents-add-High-Street-malaise-stagnating-housing-market-pushes-firms-brink.html (Accessed: 23 August 2018).

Harris Interactive (2019) *Consumer Internet of Things security labelling survey research findings*. p.3. Available at: https://assets.publishing.service.gov.uk /government/uploads/system/uploads/attachment_data/file/798543/Harris_Interactive_Consumer_IoT_Security_Labelling_Survey_Report.PDF. (Accessed: 17 February 2020).

Harris, R. and Paley, S. (2016) 'The police practitioner view' *Cybercrime workshop: Police Knowledge fund,* University of Birmingham, 19 September.

Hauptman, A. and Sharan, Y. (2013) 'Foresight of evolving security threats posed by emerging technologies', *Foresight*, 15(5), pp.375-391.

Hay, A. (2015) *The shadow internet of things – a new risk for financial services*. Available at: http://www.bankingtech.com/372591/the-shadow-internet-of-things-a-new-risk-for-financial-services/ (Accessed: 16 February 2017).

Hay Newman, L. (2019) *Hackers can break into an iPhone just by sending a text*. Available at: https://www.wired.com/story/imessage-interactionless-hacks-google-project-zero/ (Accessed 6 May 2020).

Hern, A. (2018a) *Fitness tracking app Strava gives away location of secret US army bases*. Available at:https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases. (Accessed:19 May 2020).

Hern, A. (2018b). *Cybercrime: £130bn stolen from consumers in 2017, report says*. Available at: https://www.theguardian.com/technology/2018/jan /23/cybercrime-130bn-stolen-consumers-2017-report-victims-phishing-ransomware-online-hacking (Accessed: 22 August 2018).

Hewlett Packard (2015) *Internet of Things research study: 2015 report.* Available at: http://h20195.www2.hp.com/V2/GetDocument.aspx? docname=4AA5-4759ENW&cc=us&lc=en (Accessed: 24 January 2016).

Hewlett Packard Enterprise (2016) *Josh Corman leads the drive to make 'smart' devices secure – HPE business insights*. Available at: https://www.hpe.com /h30683/us/en/strategic-business-insights/c/enterprise-security/innovation/josh-corman-leads-the-drive-to-make--smart--devices-secure.html (Accessed: 7 October 2016).

Hicks, D. (2018a) Email to Raichel Collis, 15 May.

Hicks, D. (2018b) Email to Raichel Collis, 9 October.

Hicks, D. (2019) Conversation with Raichel Collis, 30 April.

Hicks, D. (2020) Conversation with Raichel Collis, 27 May.

Higginbotham, D. (2018) *Overview of the UK's financial sector*. Available at: https://www.prospects.ac.uk/jobs-and-work-experience/job-sectors/accountancy-banking-and-finance/overview-of-the-uks-financial-sector (Accessed: 12 May 2019).

Hildenbrand, J. (2016) *Everything you need to know about rooting your Android*. Available at: http://www.androidcentral.com/root (Accessed: 4 February 2017).

HM Government (2015) *National security strategy and strategic defence review 2015*. Available at: https://www.gov.uk/government/uploads/system/uploads /attachment_data/file/478933/52309_Cm_9161_NSS_SD_Review_web_only.PDF (Accessed: 3 December 2015)

HM Government (2016) *National cyber security strategy 2016-2021*. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.PDF (Accessed: 19 December 2016).

Hodges, J. (2002) 'Internet netiquette - what is it and why is it important', *Journal of Practical Estate Planning*, 4(5), pp.11-52

Hoehle, H. and Venkatesh, V. 2015, 'Mobile application usability: conceptualization and instrument development', *MIS Quarterly*, 39, 2, pp. 435-A12, Business Source Premier, EBSCO*host*, viewed 2 February 2017.

Hoffman, C. (2013) *What's the difference between jailbreaking, rooting, and unlocking?* Available at: http://www.howtogeek.com/135663/htg-explains-whats-the-difference-between-jailbreaking-rooting-and-unlocking/ (Accessed: 4 February 2017).

Hoffman, C. (2016) *Why buying a smart fridge is a dumb idea*. Available at: https://www.howtogeek.com/260896/why-buying-a-smart-fridge-is-a-dumb-idea/ (Accessed: 15 February 2017).

Hollingsworth, S. (2019) *R.I.P. to the top 10 failed social media sites*. Available at: https://www.searchenginejournal.com/failed-social-media-sites/303421/#close (Accessed: 17 June 2020).

Hollis, M., Felson, M. and Welsh, B. (2013) 'The capable guardian in routine activities theory: A theoretical and conceptual reappraisal', *Crime Prevention and Community Safety*, 15(1), pp.65-79.

Holt, T. and Bossler, A. (2008) 'Examining the applicability of lifestyle-routine activities theory for cybercrime victimization' ,*Deviant Behaviour*, 30(1), pp.1-25.

Hooley, T., Marriott,J. and Wellens, J. (2012) *What is online research? Using the internet for social science research.* London: Bloomsbury Academic

Hopkins, M. and Dehghantanha, A. (2016) Exploit Kits: The production line of the cybercrime economy? *Second International Conference on Information Security and Cyber Forensics (Infosec)*.

Horn, P. (2006) *It's time to arrest cybercrime*. Available at: https://www.bloomberg.com/news/articles/2006-02-01/its-time-to-arrest-cybercrime (Accessed: 31 January 2017).

Hu, Y., Wang, H., Zhou, Y., Guo, Y., Li, L., Luo, B. and Xu, F. (2019) 'Dating with scambots: Understanding the ecosystem of fraudulent dating applications', *IEEE Transactions on Dependable And Secure Computing*, pp.1-1.

Huang, A. H. and Tsao, C (2015) '"Mobile" phones: the time/space and society/individual in the liquid modernity', *Mass Communication Research*, 124(0), pp. 39–81. Available at: http://search.ebscohost.com.ezproxy.derby.ac.uk/login.aspx?direct=true&db=edsdoj&AN=edsdoj.20f9200328de444d85e8fde0fcc758b7&site=eds-live (Accessed: 23 May 2020).

Huber, M., Mulazzani, M., Weippl, E., Kitzler, G., Goluch, S. (2010) 'Friend-in-the-middle Attacks', *SBA-Research-0710-01 Technical Report*. Available at: https://www.sba-research.org/wp-content/uploads/publications/FITM_TR-SBA-Research-0710-01.PDF (Accessed: 7 October 2019).

Humphries, D. (2015) *Are Millennials the latest security threat?* Available at: http://www.softwareadvice.com/security/industryview/millennial-threat-report-2015/ (Accessed: 16 February 2017).

Hunt, G. (2019) 'Social Media Platforms Double as Major Malware Distribution Centres', *TitanHQ,* 17 October. Available at: https://www.titanhq.com/blog/social-media-platforms-double-as-major-malware-distribution-centres/(Accessed: 24 March 2020).

Hunt, T. (2017) *Inside the massive 711 million record online spambot dump*. Available at: https://www.troyhunt.com/inside-the-massive-711-million-record-onliner-spambot-dump/ (Accessed: 30 August 2018).

Hurlburt, G. (2017) 'Shining light on the dark web', *Computer*, 50(4), pp. 100–105. doi: 10.1109/MC.2017.110.

Hymas, C. (2020) 'Cyberspace is unregulated 'Wild West', says MI5 chief'. Available at: http://search.ebscohost.com.ezproxy. derby.ac.uk/login.aspx?direct=true&db=edsgbe&AN=edsgcl.615169967&site=eds-live (Accessed: 23 May 2020).

ICO (2020a) *Right to erasure.* Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/(Accessed: 20 May 2020).

ICO (2020b) *Your right to get your data deleted.* Available at: https://ico.org.uk/your-data-matters/your-right-to-get-your-data-deleted/(Accessed: 20 May 2020).

iGaming Business (2020) *ACMA issues warning over scam gambling emails and texts*. Available at: https://www.igamingbusiness.com/news/acma-issues-warning-over-scam-gambling-emails-and-texts(Accessed: 19 March 2020).

Influencer Marketing Hub (2019) *Snapchat statistics and revenue. Snapchat by the numbers*. Available at: https://influencermarketinghub.com/snapchat-statistics-revenue/(Accessed: 6 April 2020).

Invision (2019) *Fake updates vs legitimate software updates.* Available at: https://invisionkc.com/software-updates/(Accessed: 23 March 2020).

IoT For All (2020) *In spite of numerous setbacks, IoT engineers are continuing to break new ground*. Available at: https://www.IoTforall.com/in-spite-of-numerous-setbacks-IoT-engineers-are-continuing-to-break-new-ground/ (Accessed 21 April 2020).

IoT Line Up (2020) *IoT devices list : Smart home devices :Top Internet of Things devices*. Available at: http://IoTlineup.com/ (Accessed: 3 February 2020).

Ivančík, R. (2020) 'Cyber threats as one of the most serious asymmetric security threats in 21st century', *Kosice Security Revue,* 10(1), pp. 10–23.

Jackson, J.T. and Creese, S. (2012) 'Virus propagation in heterogeneous bluetooth networks with human behaviours', *IEEE Transactions on Dependable and Secure Computing*, 9(6) p. 930.

Jagati, T,N., Johnson, N ,A., Jakobsen, M. and Menczer,F. (2007) 'Social phishing', *Communications of the ACM*, 50(10), pp. 94 -100.

Jawed, S. Mahboob, U. and Yasmeen, R. (2019) 'Digital professional identity: Dear Internet! Who am I?' *Brief Communication*, 32 (1) pp 33-55

Jefferson, V (2021) 'What does a 'cracked PC game' mean?' *Quora* , 11 February. Available at: https://www.quora.com/What-does-a-%E2%80%98cracked-PC-game%E2%80%99-mean/answer/Veronica-Jefferson Accessed 21 February 2021

Jeske, D. and van Schaik, P. (2017) 'Familiarity with internet threats: Beyond awareness', *Computers and Security*, 66, pp. 129–141. doi: 10.1016/j.cose. 017.01.010.

Johansen, A.G. (2020) *Is jailbreaking legal and safe?* Available at: https://us.norton.com /internetsecurity-mobile-is-jailbreaking-legal-and-safe.html (Accessed: 25 July 2020).

Johnson, J. (2020) *Social media usage in the United Kingdom (UK) - Statistics and Facts.* Available at: https://www.statista.com/topics/3236/social-media-usage-in-the-uk/ (Accessed: 6 June 2020).

Johnson, M. (2016) *Shadow data report*. Available at: http://images.machspeed.bluecoat.com/Web/BlueCoat/%7B2f3a44c7-7445-442a-9425-de48041ab3c9%7D_ShadowDataReport_1H_2016_Digital-Screen_compressed.PDF (Accessed: 8 February 2017).

Johnston, A. C., Warkentin, M. and Siponen, M. (2015) 'An enhanced fear appeal rhetorical framework: Leveraging threats to the human asset through sanctioning rhetoric', *MIS Quarterly*, 39(1), pp. 113-134.

Jones, R. (2016) *Mobile banking on the rise as payment via apps soars by 54% in 2015*. Available at: https://www.theguardian.com/business/2016/jul/22/mobile-banking-on-the-rise-as-payment-via-apps-soars-by-54-in-2015 (Accessed: 17 September 2018).

Jones, R. (2020) *Best smart plugs 2020: add intelligence to any power socket*. Available at: https://www.t3.com/features/best-smart-plugs (Accessed: 8 February 2020).

Jordan, K. (2020) 'Imagined audiences, acceptable identity fragments and merging the personal and professional: How academic online identity is

expressed through different social media platforms', *Learning, Media and Technology,* 45 (2) pp. 165-178

Juba, S. and Young, D. (2018) *Be mindful of your digital footprint.* Available at: http://www.sbnonline.com/article/mindful-digital-footprint/ (Accessed: 24 August 2018).

Junger, M., Montoya, L. and Overink, F. (2017) 'Priming and warnings are not effective to prevent social engineering attacks', *Computers in Human Behavior*, 66, pp. 75–87. doi: 10.1016/j.chb.2016.09.012.

Junior, D, M., Melo, L., Lu, H., Amorim, M. and Prakash, A. (2019) 'Beware of the app! On the vulnerability surface of smart devices through their companion apps', Available at: http://arxiv.org/abs/1901.10062 (Accessed: 11 February 2020).

Kan, M. (2020) *New bug hacks android devices via bluetooth.* Available at: https://www.pcmag.com/news/new-android-bug-exploits-bluetooth-to-hack-the-device (Accessed 18 June 2020).

Kaplan, O. (2019) *Mobile gaming is a $68.5 billion global business, and investors are buying in*. Available at: https://techcrunch.com/2019/08/22/mobile-gaming-mints-money/(Accessed: 16 March 2020).

Kapuria, S. (2008) 'IT risk and the millennials', *Tech Decision Maker*, 22 January Available at: https://www.techrepublic.com /index. php/blog/tech-decision-maker/it-risk-and-the-millennials/ (Accessed 12 March 2017).

Karnes, K.C. (2019) ‘Why Users Uninstall Apps: 28% of People Feel Spammed’, *Clevertap,* 04 April. Available at: https://clevertap.com/blog/uninstall-apps/#infographic (Accessed: 21 December 2019).

Kaspersky (2016) *Implementation techniques*. Available at: http://usa.kaspersky.com/internet-security-center/threats/malware-implementation-techniques#.WCm5RCSMQ2w (Accessed: 14 November 2016).

Kaspersky (2019a) *Game of threats: How cybercriminals use popular TV shows to spread malware*. Available at: https://securelist.com/game-of-threats/90116/ (Accessed: 01 November 2019).

Kaspersky (2019b) ‘Wi-Fi In the Office - Convenient But Risky’, *Kaspersky Blog*, 11 June. Available at: https://www.kaspersky.com/blog/vulnerable-wi-fi/27250/(Accessed: 22 December 2019).

Kaspersky (2020) *You got a match! With a cyber-criminal* [Press release] 12 February. Available at: https://www.kaspersky.com/about/press-releases/2020_you-got-a-match-with-a-cyber-criminal (Accessed: 19 March 2020).

Kaspersky (2021) *What are Cookies?* Available at: https://www.kaspersky.com/

resource-center/definitions/cookies. (Accessed 25 January 2021).

Kearnes, M. (2008) ‘Risk Society: Towards a new modernity by Ulrich Beck’, *Geography*, 93 (2) pp. 122–123.

Kember, R. (2018) Email to Raichel Collis, 26 June.

Kemp, S. (2020) *Digital 2020: global digital yearbook*. Available at: https://p.widencdn.net/1zybur/Digital2020Global_Report_en (Accessed 21 June 2020).

Kemper, G. (2018 a) *Do wearable devices connect people to the Internet of Things?* Available at: https://clutch.co/it-services/resources/wearables-connect-internet-of-things-technology (Accessed:21 February 2020).

Kemper, G. (2018 b) *How people use connected devices.* Available at: https://clutch.co/it-services/resources/how-people-use-connected-devices (Accessed: 14 February 2020).

Kelion, L. (2014) *Apple toughens iCloud security after celebrity breach - BBC News*. Available at: http://www.bbc.com/news/technology-29237469 (Accessed: 8 July 2017).

Kerstens, J. and Jansen, J. (2016) 'The victim – perpetrator overlap in financial cybercrime: Evidence and reflection on the overlap of youth's on-line victimization and perpetration', *Deviant Behavior*, 37(5), pp. 585–600. doi: 10.1080/01639625.2015.1060796.

Khamis, S., Ang, L. and Welling, R. (2017) 'Self-branding, 'micro-celebrity' and the rise of social media influencers,' *Celebrity Studies*, 8(2), pp. 191-208 DOI: 10.1080/19392397.2016.1218292

Khan, R., Kumar, P. Jayakody, D.N. and Liyange, M. (2019 'A survey on security and privacy of 5g technologies: Potential solutions, recent advancements, and future directions', *IEEE Communications Surveys and Tutorials,* 22 (1), pp. 196–248. doi: 10.1109/COMST.2019.2933899.

Kigoulis, L. (2017) *What are SPAM tools and how to remove them.* 2-spyware.com. Available at: https://www.2-spyware.com/spam-tools-removal#qm-h2-1 (Accessed: 28 August 2018).

Kim, H., Lee, J. and & Oh, S. (2019). 'Individual characteristics influencing the sharing of knowledge on social networking services: online identity, self-efficacy, and knowledge sharing intentions', *Behaviour and Information Technology*. 39 (2) pp.1-12.

Kinzie, K. (2020) '7 Wi-Fi Security Tips: Avoid Being Easy Prey for Hackers', *Inside Out Security*, 29 March. Available at: https://www.varonis.com/blog/7-wi-fi-security-tips-avoid-being-easy-prey-for-hackers/(Accessed: 9 April 2020).

Knight, L. (2015) 'Black swan events', *The Strategic CFO*, 27 February Available at https://strategiccfo.com/black-swan-events/ (Accessed: 26 June 2019).

KnowBe4 (2017) *Phishing* | *common phishing scams*. Available at: http://www.phishing.org/common-phishing-scams (Accessed: 8 Jul. 2017).

Kobie, N. (2015) *Get yourself connected: Is the Internet of Things the future of fashion?* Available at: https://www.theguardian.com/technology/ 2015/apr /21/internet-of-things-future-fashion (Accessed: 13 February 2017).

Koch, W. (2008) *Sexual predators prowl new outlet*. Available at: http://link.galegroup.com /apps /doc/A180897403/ITOF?u =derby&sid=ITOF&xid=8823763f. (Accessed: 22 September 2018).

Kohler, C. (2019) *Here are the 7 Reasons Why LinkedIn is important*. Available at: https://www.topresume.com/career-advice/why-linkedin-is-important (Accessed: 21 October 2019).

Kokh, M.T. (2019) 'Symantec Mobile Threat Defense: A Snapshot of Mobile Security Incidents in Q1 2019'. *Symantec Enterprise*, 1 April . Available at: https://symantec-enterprise-blogs.security.com/blogs/product-insights/symantec-mobile-threat-defense-snapshot-mobile-security-incidents-q1-2019 (Accessed 6 May 2020).

Kounalakis, M. (2018) 'The mayor of tech territory: Cyberspace is often compared to the Wild West--but eventually the west was won, and the frontier tamed. It's time for our virtual villages to get civilized', *Hoover Digest*, (4), p. 84. Available at: http://search.ebscohost.com.ezproxy.derby.ac.uk/login.aspx?direct=true&db=edsgov&AN=edsgcl.569457563&site=eds-live (Accessed: 23 May 2020).

Kraemer, S., Carayon, P. and Clem, J. (2009) 'Human and organizational factors in computer and information security: Pathways to vulnerabilities', *Computers and Security*, 28(7), pp. 509–520. doi: 10.1016/j.cose.2009.04.006.

Krotoski, A (2017) *Aleks in Wonderland,* BBC Radio 4, 30 August. Available at: http://www.bbc.co.uk/programmes/b092fszv (Accessed: 29 November 2017).

Krug, R.(2019) '4 Ways the WhatsApp Exploit Could Use Employees to Infiltrate Your Network', *Sonicwall*, 17 May. Available at: https://blog.sonicwall.com/en-us/2019/05/4-ways-the-whatsapp-exploit-could-use-employees-to-infiltrate-your-network/(Accessed: 6 April 2020).

Kumaraguru, P. Sheng, S. Acquisti, A. Cranor, L. and Hong, J. (2008) 'Lessons from a real-world evaluation of anti-phishing training', *Ecrime Researchers Summit*, p.1, Publisher Provided Full Text Searching File, EBSCO*host*, viewed 16 February 2017.

Kumaraguru, P., Cranshaw, J., Acquisti, A., Cranor, L., Hong, J., Blair, M.A. and Pham, T. (2009) 'School of phish: a real-world evaluation of anti-phishing training', *Proceedings of the 5th Symposium on Usable Privacy and Security - SOUPS '09*, doi: 10.1145/1572532.1572536.

Kunsman, T. (2018) *Why you need to develop a powerful personal brand identity at work* Available at: https://everyonesocial.com/blog/personal-brand-identity/ (Accessed: 21 October 2019).

Lake, L. (2019)*Tips on creating and growing your personal brand*. Available at: https://www.thebalancesmb.com/creating-and-growing-personal-brand-2295814 (Accessed: 21 October 2019).

Landman, F. (2019) *Is IoT dead? Why IoT is changing and how it lives on*. Available at: https://readwrite.com/2019/01/16/is-IoT-dead-why-IoT-is-changing-and-how-it-lives-on/ (Accessed 21 April 2020).

Landesman, M. (2018) *Think your email may have been hacked? Read this.* Available at: https://www.lifewire.com/help-my-email-was-hacked-153284 (Accessed: 4 September 2018).

Lane, S. (2014) *How private browsing settings actually work*. Available at: https://mashable.com/2014/07/21/how-private-browsing-works/?europe=true#BCxGfCz6W8qO (Accessed: 18 September 2018).

Langley, H. (2020) *Smart hearables go beyond the music at CES 2020: Here are the best.* Available at: https://www.techradar.com/news/smart-hearables-go-beyond-the-music-at-ces-2020-here-are-the-best (Accessed: 9 May 2020).

Lanier, J. (2018) *Ten arguments for deleting your social media accounts right now.* Available at http://www.amazon.co.uk/kindlestore (Downloaded: 17 July 2018).

Laplan, S. D., Quartaroli, M.T. and Riemer, F.J (2012) Introduction to qualitative Research, in Laplan, S. D., Quartaroli,M.T. and Riemer,F.J. (eds) *Qualitative research: an introduction to methods and designs***,** Jossey-Bass, San Francisco, California.

Lapsley, P. (2013) *Exploding the phone*. New York, NY Grove Press.

La Porta, L. (2018) *Discontinued apps - apps that are outliving their developers*. Available at: https://www.wandera.com/discontinued-apps/ (Accessed: 28 January 2020).

Lastline (2019)' Cloud Data Security – 5 Attacks to Watch For In 2019', *Lastline*, 8 January. Available at: https://www.lastline.com/blog/cloud-data-security-5-attacks-to-watch-for-in-2019 (Accessed: 10 June 2020).

Laughlin, A. (2020) *Smart toys - should you buy them?* Available at: https://www.which.co.uk/reviews/toys/article/smart-toys-should-you-buy-them. (Accessed: 27 February 2020).

Lee, D. (2017) *Defending Tor - gateway to the dark web*. Available at: https://www.bbc.co.uk/news/technology-40810771 (Accessed 8 June 2020).

Lee, D. (2019) *WhatsApp discovers surveillance attack*. Available at: https://www.bbc.co.uk/news/technology-48262681(Accessed: 6 April 2020).

Lee, J., de Guzman, M., Talebi, N., Korni, S., Szumigala, D. and Rao, H. (2018). 'Use of online information and suitability of target in shoplifting: A routine activity-based analysis', *Decision Support Systems*, 110, pp.1-10.

Leukfeldt, E. (2014) 'Cybercrime and social ties', *Trends in Organized Crime*, doi: 10.1007/s12117-014-9229-5.

Leukfeldt, E. and Yar, M. (2016) 'Applying routine activity theory to cybercrime: A theoretical and empirical analysis', *Deviant Behavior*, 37(3), pp.263-280.

Leukfeldt, E.R., Kleemans, E.R. and Stol, W.P. (2017) 'Cybercriminal networks, social ties and online forums: social ties versus digital ties within phishing and malware networks'. *British Journal of Criminology*, 57(3), pp. 704-722.

Lewis, R. (2019) 'Readers Comments', *Technobezz*, 26 September. Available at: https://www.technobezz.com/5-reasons-keep-apps-date/ (Accessed: 28 October 2019).

Li, Y., Wang, H. and Sun, K. (2017) ‘Personal information in passwords and its security implications’, *IEEE transactions on information forensics and security*, 12(10), pp.2320-2333.

Liang, N., Biros, D. P. and Luse, A. (2016) ‘An empirical validation of malicious insider characteristics’, *Journal of Management Information Systems*, 33(2), pp. 361–392. doi: 10.1080/07421222.2016.1205925.

Lindemann, N. (2019) ‘What’s the average survey response rate? (2019 benchmark), *Survey Anyplace,* 8 August. Available at: https://surveyanyplace.com /average-survey-response-rate/(Accessed: 25 June 2020).

Ling, Z., Luo, J., Xu, Y., Gao, C., Wu, K. and Fu, X. (2017) ‘Security vulnerabilities of internet of things: A case study of the smart plug system’, IEEE *Internet of Things Journal*, 4(6), pp.1899-1909.

LinkedIn (2019) *Enabling and managing the ‘open to job opportunities’ feature on your LinkedIn profile*. Available at: https://www.linkedin.com/help/linkedin/answer/ 110869?query=Show%20recruiters%20you%E2%80%99re%20open%20to%20job%20opportunities&hcppcid=search (Accessed: 21 October 2019).

Lister, M. (2020) ‘37 Staggering Video Marketing Statistics for 2018’, *Wordstream,* 20 June. Available at: https://www.wordstream.com/blog/ws/2017/03/08/video-marketing-statistics (Accessed 7 July 2020).

Liu, J. and Sun, W. (2016) ‘Smart attacks against intelligent wearables in people-centric Internet of things’, *IEEE Communications Magazine*, 54(12), pp. 44–49. doi: 10.1109/mcom.2016.1600553cm.

Liu, L. (2020) *Internet of Things*. Available at: https://www.statista.com/topics /2637/internet-of-things/(Accessed: 9 May 2020).

Lohn, A. J. (2018) 'Timelines for in-code discovery of zero-day vulnerabilities and supply-chain attacks'. Available at: http://search.ebscohost.com.ezproxy. derby.ac.uk/login.aspx?direct=true&db=edsarx&AN=edsarx.1808.10062&site=eds -live (Accessed: 9 June 2020).

Long, C. (2015) *Four in five apps' web scripting languages fail industry-standard security benchmark*. Available at: http://business-reporter.co.uk/2015/12/04/four-in-five-applications-web-scripting-languages-fail-industry-standard-security-benchmark/ (Accessed: 4 December 2015).

Look, J. (1999) 'The virtual wild, wild west (www): Intellectual property issues in cyberspace—trademarks, service marks, copyrights, and domain names'*. Bowen Law Repository: Scholarship and Archives*. Available at: http://lawrepository. ualr.edu/lawreview/vol22/iss1/4 (Accessed: 09 August 2018).

Lord, N. (2020) 'What is Polymorphic Malware? A Definition and Best Practices for Defending Against Polymorphic Malware', *Data Insider*, 17 July. Available at: https://digitalguardian.com/blog/what-polymorphic-malware-definition-and-best-practices-defending-against-polymorphic-malware (Accessed 13 March 2021).

Loterina, C. (2016) *Google confirmed to release Android wear 2.0 Smartwatches: Here's what to expect from the Wearable OS*. Available at: http://www.techtimes. com /articles/189954/20161223/google-confirmed-to-release-android-wear-2-0-

smartwatches-heres-what-to-expect-from-the-wearable-os.htm (Accessed: 13 February 2017).

Lovink, G. and Rossiter, N. (2009) 'The digital given: 10 web 2.0 theses', *The Fibreculture Journal*. Available at http://fourteen.fibreculturejournal.org/fcj-096-the-digital-given-10-web-2-0-theses/ (Accessed: 27 January 2017).

Lutrum (2019) 'New malware is coming through messaging apps' *Lutrum LLC,* 19 March. Available at: https://www.lutrum.com/2019/03/19/new-malware-is-coming-through-messaging-apps/(Accessed: 24 March 2020).

Lumb, D. (2019) *Here's what experts say mobile gaming will look like in 2020*. Available at: https://www.techradar.com/uk/news/mobile-gaming-trends-2020 (Accessed: 17 March 2020).

Lyall Grant, L. (2016) Interviewed by Jane Garvey for BBC Radio 4 Woman's Hour, 23 November. Available at http://www.bbc.co.uk/programmes/b082vyzr (Accessed: 25 November 2016)

Lynch, G. (2020) *New to smart assistants?* Available at: https://www.realhomes.com/advice/smart-assistants (Accessed: 3 February 2020).

Lyng, S. (2005). *Edgework : the sociology of risk-taking*. New York and London: Routledge.

MacDonald, W. (2019) *Financial services need to bank on secure instant messaging*. Available at: https://www.business2community.com/finance/financial-

services-need-to-bank-on-secure-instant-messaging-02202586 (Accessed 5 May 2020).

Madden, M., Fox, S., Smith, A. and Vitak, J. (2007) *Digital footprints*. Pew Research Centre: Internet, Science and Tech. Available at: http://www.pewinternet.org/2007/12/16/digital-footprints/ (Accessed: 15 August 2018).

Maimon, D., Kamerdze, A., Cukier, M. and Sobesto, B. (2013) 'Daily trends and origin of computer-focused crimes against a large university computer network: an application of the routine-activities and lifestyle perspective', *British Journal of Criminology*, 53(2), pp.319-343.

Mansfield-Devine, S. (2008) 'Anti-social networking: Exploiting the trusting environment of web 2.0', *Network Security*, 2008(11), pp. 4–7. doi: 10.1016/s1353-4858(08)70127-2.

Mansfield-Devine, S. (2016) 'DDoS goes mainstream: How headline-grabbing attacks could make this threat an organisation's biggest nightmare', *Network Security*, 2016(11), pp. 7–13. doi: 10.1016/s1353-4858(16)30104-0.

Markham, A., and Buchanan, E. (2012) 'Ethical decision-making and internet research': *Recommendations from the AOIR Ethics Working committee* (version 2.0). Available at http://www.aoir.org/reports/ethics2.pdf. (Accessed 20 June 2020).

Martin, J. (2018) *Avoid these common Snapchat scams*. Available at: https://www.techadvisor.co.uk/how-to/social-networks/how-avoid-common-snapchat-scams-3676895/ (Accessed: 6 April 2020).

Masabo, E., Kaawaase, K.S., Sansa-Otim, J., Ngubiri, J. and Hanyurwimfura, D. (2018) ‘A state of the art survey on polymorphic malware analysis and detection techniques’, *ICTACT Journal on Soft Computing*, 8(4), pp. 1762–1774.

Matook, S., Cummings, J. and Bala, H. (2015) ‘Are you feeling lonely? The impact of relationship characteristics and online social network features on loneliness’, *Journal of Management Information Systems*, 31(4), pp. 278–310. doi: 10.1080/07421222.2014.1001282.

Matthews, D. (2016) *What makes criminal hackers want to hack?* Available at: http://raconteur.net/technology/what-makes-criminal-hackers-want-to-hack (Accessed: 8 December 2016).

Matza, D. (2010) *Becoming deviant.* Rev edn. Introduction by Thomas G Blomberg. New Brunswick and London: Transaction Publishers

Mayhorn, C.B., Murphy-Hill, E., Zielinska,O.A. and Welk, A.K. (2015) ‘The social engineering behind phishing’, *The Next Wave,* 21 pp. 24–31

McAfee (2008) *McAfee virtual criminology report*. Available at: http://www.cs.utsa.edu/~bylander/cs1023/mcafee_vcr_us.PDF (Accessed: 30 January 2017).

McAfee (2018) *McAfee Labs threat report, June 2018*. Available at: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-jun-2018.PDF (Accessed: 31 August 2018).

McAfee (2019) *Mobile threat report, Q1 2019.* Available at: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-mobile-threat-report-2019.PDF (Accessed: 12 December 2019).

McAfee (2020) *Mobile threat report*, *Q1 2020*. Available at: https://www.mcafee.com/content/dam/consumer/en-us/docs/2020-Mobile-Threat-Report.PDF (Accessed: 19 March 2020).

McCusker, R. (2007) 'Transnational organised cybercrime: Distinguishing threat from reality', *Crime, Law and Social Change*, 46(4-5), pp. 257–273. doi: 10.1007/s10611-007-9059-3.

McGrath, M. and Casey, E. (2002) 'Forensic psychiatry and the internet: practical perspectives on sexual predators and obsessional harassers in cyberspace', *Journal of the American Academy of Psychiatry and the Law Online*, 30(1), pp.81-94.

McGuire, M. (2019) *Social media platforms and the cybercrime economy. Bromium web of profit social platforms report*. Available at: https://www.bromium.com/resource/report-social-media-platforms-and-the-cybercrime-eonomy/?utm_source=Website&utm_medium=Blog&utm_campaign=WoPSocialPlatforms# (Accessed: 22 September 2019).

McMillan, R. (2010) *1.5 Million stolen Facebook IDs up for sale*. Available at: http://www.pcworld.com/article/194843/article.html (Accessed: 9 February 2017).

McRobert, C.J., Hill, J.C., Smale, T., Hay, E.M. and van der Windt, D.A. (2018) 'A multi-modal recruitment strategy using social media and internet-mediated

methods to recruit a multidisciplinary, international sample of clinicians to an online research study', *PLOS ONE*, 13, (7) https://search-ebscohost-com.ezproxy.derby.ac.uk/ login.aspx?direct=true&db=edswsc&AN= 000437809500073&site=eds-live.

Mechling, G. (2019) *IoT - A beginner's guide to making your own devices from scratch*. Available at: http://nilhcem.com/IoT/make-your-own-devices-from-scratch (Accessed: 22 February 2020).

Mesch, G.S. (2012) 'Is online trust and trust in social institutions associated with online disclosure of identifiable information online?', *Computers in Human Behavior*, 28(4), pp. 1471–1477. doi: 10.1016/j.chb.2012.03.010.

Micheli, M., Lutz, C. and Büchi, M. (2018) 'Digital footprints: An emerging dimension of digital inequality', *Journal of Information, Communication and Ethics in Society*, 16(3), p. 242. Available at: http://search.ebscohost.com.ezproxy.derby.ac.uk/login.aspx?direct=true&db=edb&AN=133000228&site=eds-live (Accessed: 18 May 2020).

Microsoft (2018) *Malware infection sources - Windows defender security intelligence*. Available at: https://www.microsoft.com/en-us/wdsi/help/malware-infection-sources (Accessed: 26 August 2018).

Microsoft (2019) 'Corporate IoT - A Path to Intrusion'*, Microsoft Security Response Centre*, August 5. Available at: https://msrc-log.microsoft.com/2019/08/05/ corporate-IoT-a-path-to-intrusion/ (Accessed: 15 February 2020).

Midlands Fraud Forum (2014) *Our mission statement*. Available at: http://www.midlandsfraudforum.co.uk/About-Us (Accessed: 16 May 2019).

Miessler, D., Guzman, A., Rudresh, V. and Smith, C. (2019) *Open web application security project Internet of Things.* Available at: https://owasp.org/www-project-internet-of-things/ (Accessed: 5 February 2020).

Miller, C. (2018) A New Type of Criminal. *The Sunday Times Magazine*, pp.14-20.

Minister for Digital and Broadband (2020) *Government response to the "Regulatory proposals for consumer Internet of Things (IoT) security" consultation*. Available at www.gov.uk/official-documents (Accessed: 17 February 2020).

Mintel Group Ltd (2016a) *Brits step up to wearable technology: Sales of fitness bands and smartwatches up 118% in 2015.* Available at: http://www.mintel.com/press-centre/technology-press-centre/brits-step-up-to-wearable-technology-sales-of-fitness-bands-and-smartwatches-up-118-in-2015 (Accessed: 29 November 2016).

Mintel Group Ltd (2016b) *Europe 17. Consumer trends 2017*. Available at: http://www.mintel.com/en/PDF/european-consumer-trends-2017.PDF (Accessed: 29 November 2016).

Miorandi, D., Sicari, S., De Pellegrini, F. and Chlamtac, I. (2012) 'Internet of things: Vision, applications and research challenges', *Ad Hoc Networks*, 10(7), pp. 1497–1516. doi: 10.1016/j.adhoc.2012.02.016.

Miró, F. (2014) 'Routine activity theory' in Mitchell Miller, J. (ed.) *The encyclopaedia of theoretical criminology*. Blackwell Publishing Ltd. Available at

https://onlinelibrary.wiley.com/action/showCitFormats?doi=10.1002%2F9781118517390.wbetc198 (Accessed: 09 July 2018).

Mitchell, B. (2019) *How to set up guest wi-fi for your home.* Available at: https://www.lifewire.com/guest-network-for-home-tutorial-818204 (Accessed:19 February 2020).

Mitnick, K. (2001) 'Telecom system security', in Anderson, R.J. (ed.) *Security engineering: A guide to building dependable distributed systems.* John Wiley and Sons.

Mittal, S. and Sharma, P. (2017) 'Enough law of horses and elephants debated.... let's discuss the cyber law seriously', *International Journal of Advanced Research in Computer Science*, 8(5), pp.1343 - 1348.

'Mobile App' (2019) *Wikipedia.* Available at: https://en.wikipedia.org/wiki/Mobile app (Accessed: 28 October 2019).

Moon, K. and Blackman, D. (2014) 'A guide to understanding social science research for natural scientists', *Conservation Biology*, 28(5), p. 1167. Available at: https://search-ebscohost-com.ezproxy.derby.ac.uk/login.aspx?direct=true&db=edsjsr& AN=edsjsr.244 80366&site=eds-live (Accessed: 10 July 2020).

Moore, M. (2019) *Plenty of Fish leaks private user information*. Available at: https://www.techradar.com/uk/news/plenty-of-fish-leaks-private-user-information (Accessed: 19 March 2020).

Moreau, E. (2016) *How to use hashtags on all your favourite social networking sites*. Available at: https://www.lifewire.com/hashtag-on-instagram-Facebook-twitter-tumblr-3486025 (Accessed: 9 August 2017).

Morse, A. (2018) '*Investigation: WannaCry cyber-attack and the NHS*', National Audit Office, pp.1 -30. Available at: https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.PDF. (Accessed: 29 Oct. 2019).

Morris, S. (2004) *The future of netcrime now: Part 1 – threats and challenges*. Available at: http://globalinitiative.net/wp-content/uploads/2017/01/the-future-of-netcrime-now-part-1-threats-and-challenges.PDF (Accessed: 30 January 2017).

Morris, S. (2014) *Study finds social media use beneficial to overall health of elderly*. Available at: https://www.theguardian.com/media/2014/dec/12/study-finds-social-media-skype-facebook-use-beneficial-overall-health-elderly (Accessed: 27 January 2017).

Moser, S., Bruppacher, S.E. and Mosler, H.-J. (2010) 'How people perceive and will cope with risks from the diffusion of ubiquitous information and communication technologies', *Risk Analysis*, 31(5), pp. 832–846. doi: 10.1111/j.1539-6924.2010.01544.x.

Mouton, F., Leenen, L., Malan, M.M. and Venter H. S. (2014) 'Towards an ontological model defining the social engineering domain' *ICT and Society*, Springer pp. 266–279

Mouton, F., Leenen, L. and Venter, H.S. (2016) ‘Social engineering attack examples, templates and scenarios’, *Computers and Security*, 59, pp. 186–209. doi: 10.1016/j.cose.2016.03.004.

Moyle, E. (2016) *Three steps to better security in IoT devices*. Available at: http://internetofthingsagenda.techtarget.com/tip/Three-steps-to-better-IoT-device-security-in-the-enterprise (Accessed: 15 February 2017).

Murdock, J. (2016) *Apple iOS vs Google Android: Which is the more secure smartphone OS?* Available at: http://www.ibtimes.co.uk/apple-ios-vs-google-android-which-more-secure-smartphone-os-1547396 (Accessed: 9 December 2016).

Mutchler, A. (2018)*A timeline of voice assistant and smart speaker technology From 1961 to today* Available at: https://voicebot.ai/2018/03/28/timeline-voice-assistant-smart-speaker-technology-1961-today/(Accessed 6 July 2021).

Myers, L.(2015) *Security terms explained: What does Zero Day mean?* Available at: ttps://www.welivesecurity.com/2015/02/11/security-terms-explained-zero-day-mean/(Accessed 23 July 2020).

Nagasamy, A. (2019) ‘Can We Enable Wi-Fi and Mobile Data Both at the Same Time On an Android Device and Communicate Simultaneously?’ *Quora,* 13 April. Available at: https://www.quora.com (Accessed: 21 February 2020).

Natanson, E. (2019) *The "other" Android app stores - a new frontier for app discovery*. Available at: https://www.forbes.com/sites/eladnatanson /2019/09/03/ the-other-android-app-stores-a-new-frontier-for-app-discovery/#5e5830f96774 (Accessed: 1 November 20

National Communications System (2000) *The electronic intrusion threat to national security and emergency preparedness (NS/EP).* Internet Communications, Diane Publishing.

NCSC National Cyber Security Centre (2018a) *10 steps to cyber security.* Available at: https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security/introduction-to-cyber- security/common-cyber-attacks-reducing-the-impact (Accessed:15 May 2020).

NCSC National Cyber Security Centre (2018b) *10 steps to cyber security: User education and awareness.* Available at: https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security/the-10-steps/user-education-and-awareness (Accessed:15 May 2020).

Neave, N., Briggs, P., McKellar, K. and Sillence, E. (2019) 'Digital hoarding behaviours: Measurement and evaluation', *Computers in Human Behavior*, 96, pp.72-77.

Neild, B., Wilson, N., Dell 'Atti, A., Sansonetti, S. and Brodolini, F.G. (2014) *Activating and guiding the engagement of seniors through social media.* Final Report. Available at: http://ages2.eu/sites/default/files/page/Ages-final-report-EN.PDF (Accessed: 25 November 2016).

Newman, L.H. (2018) *Pop-up mobile ads surge as sites scramble to stop them*. Available at: https://www.wired.com/story/pop-up-mobile-ads-surge-as-sites-scramble-to-stop-them/ (Accessed: 6 July 2020)

Newman, L.H. (2019a) *How hackers broke WhatsApp with just a phone call*. Available at: https://www.wired.com/story/whatsapp-hack-phone-call-voip-buffer-overflow/ (Accessed: 5 April 2020).

Newman, L.H. (2019b) *How to check your computer for hacked ASUS software update.* Available at: https://www.wired.com/story/asus-software-update-hack/ (Accessed: 17 September 2019).

Nield, D. (2019) *How to add voice control to all of your smart home devices*, *Popular Science.* Available at: https://www.popsci.com/how-to-add-voice-control-alexa-google-assistant-siri/ (Accessed: 7 February 2020).

Netnames (no date) *Cyberlocker door: A report on how shadowy Cyberlocker businesses use credit card companies to make millions*. Available at: https://www.netnames.com/assets/shared/whitepaper/PDF/dca-netnames-cyber-profibility-1.compressed.PDF (Accessed: 8 February 2017).

Nikas, A., Alepis, E. and Patsakis, C. (2018) 'I know what you streamed last night: On the security and privacy of streaming', *Digital Investigation*, 25, pp.78-89.

No, J. (2019) *How to get noticed on LinkedIn by recruiters.* Available at: https://www.atriumstaff.com/get-noticed-linkedin/(Accessed: 21 October 2019).

Nodegraph (2020) *How much data is on the internet? The big data facts update 2020.* Available at: https://www.nodegraph.se/how-much-data-is-on-the-internet/ (Accessed 19 July 2020).

Nokia (2016) *Threat intelligence Report – H1*. Available at: https://nokiamob.net/wp-content/uploads/2016/09/Nokia-TI-Report-H1-2016.pdf (Accessed 12 January 2017).

Norton (2018) *What is spyware? And how to remove it*. Available at: https://us.norton.com/internetsecurity-how-to-catch-spyware-before-it-snags-you.html (Accessed: 24 June 2020).

Norton (2019) *What is a digital footprint? And how to help protect it from prying eyes*. Available at: https://us.norton.com/internetsecurity-privacy-clean-up-online-digital-footprint.html (Accessed: 20 May 2020).

Norton (2020) *12 tips to secure your smart home and IoT devices.* Available at: https://us.norton.com/internetsecurity-IoT-smart-home-security-core.html (Accessed: 20 February 2020).

Numaan, H., Hilt, S. and Hellberg, N. (2017) 'What's in Shodan? Analyzing Exposed Cyber Assets in The United States', *TrendLabs,* 15 February. Available at: http://blog.trendmicro.com/trendlabs-security-intelligence/whats-shodan-analyzing-exposed-cyber-assets-united-states/ (Accessed: 16 February 2017).

O'Donnell, A. (2020) *What is clickbait? You'll be shocked by what's really going on*! Available at: https://www.lifewire.com/the-dark-side-of-clickbait-2487506 (Accessed: 12 July 2020).

Odorčák, J. (2019) 'Exorganic posthumanism and brain-computer interface technologies', *Postmodern Openings / Deschideri Postmoderne*, 10(4), pp.193–208. doi: 10.18662/po/103.

OECD (2020) *Enterprises by business size (Indicator).* Available at: https://data.oecd.org/entrepreneur/enterprises-by-business-size.htm (Accessed: 25 January 2020).

Ofcom (2017) *Rise of the social seniors revealed*. Available at: https://www.ofcom.org.uk/about-ofcom/latest/features-and-news/rise-social-seniors (Accessed: 23 August 2018).

Ofcom (2018) *Adults' media use and attitudes report 2018*. Ofcom. Available at: https://www.ofcom.org.uk/research-and-data/media-literacy-research/adults/adults-media-use-and-attitudes (Accessed: 23 Aug. 2018).

Ofcom (2019) *Adults: Media use and attitudes report (2019)* Available at: https://www.ofcom.org.uk/research-and-data/media-literacy-research/adults/adults-media-use-and-attitudes (Accessed: 15 May 2020).

Office of the Privacy Commissioner of Canada (2017) *Privacy Enhancing Technologies – A Review of Tools and Techniques.* Available at: https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2017/pet_201711/#heading-0-0-15 (Accessed: 24 June 2021).

ONS Office for National Statistics (2019) *Internet users, UK: 2019*. Available at: https://www.ons.gov.uk/businessindustryandtrade/itandinternetindustry/bulletins/internetusers/2019 (Accessed 25 February 2021).

Ohana, D. and Shashidhar, N. (2013) 'Do private and portable web browsers leave incriminating evidence? A forensic analysis of residual artefacts from private

and portable web browsing sessions', *EURASIP Journal on Information Security*, 2013(1).

Omand, D., Bartlett, J. and Miller, C. (2012) 'Introducing Social Media Intelligence (SOCMINT), *Intelligence and National Security*, 27(6), pp.801-823.

OpenDNS (2015) *Open DNS 2015 IoT report*. Available at: http://info.opendns.com/rs/033-OMP-861/images/OpenDNS-2015-IoT-Report.PDF (Accessed: 18 December 2015).

Orman, L.V. (2013) 'Technology as risk', *IEEE Technology and Society Magazine* pp. 22–31.

Ormerod, K. (2018) 'Confessions of an influencer', *The Sunday Times Style Magazine* (September), pp. 38-39.

Osborne, C. (2020) *WolfRAT targets WhatsApp, Facebook Messenger app users on Android devices*. Available at: https://www.zdnet.com/article/wolfrat-targets-users-of-whatsapp-facebook-messenger-apps-on-android-devices/.(Accessed: 18 June 2020).

Otey, B.S. (2013) 'Millennial's, technology and professional responsibility: Training a new generation in technological professionalism', *Journal of the Legal Profession*, 37(2), pp. 199–264.

Ovadya, A., Ogen, R., Mallah, Y., Gilboa, N. and Oren, Y. (2019) 'Cross-router covert channels', *13th USENIX Workshop on Offensive Technologies*, Santa Clara, CA, 12 August to 13 August 2019.

Paganini, P. (2016) *Zero-day exploits in the dark*. Available at: http://resources.infosecinstitute.com/zero-day-exploits-in-the-dark/ (Accessed: 7 December 2016).

Paganini, P. (2019) *What are the risks for average users who download content via torrent*. Available at: https://resources.infosecinstitute.com/torrent-content-downloading-risks/ (Accessed: 8 November 2019).

Pak, J. and Park, K. (2012) 'UbiMMS: An ubiquitous medication monitoring system based on remote device management methods', *Health Information Management Journal*, 41(1), pp. 26–30. doi: 10.1177/183335831204100104.

Palmer, D. (2017a) *Facebook Messenger user? Watch out for fake messages rigged with malware.* Available at: https://www.zdnet.com/article/facebook-messenger-user-watch-out-for-fake-messages-rigged-with-malware/ (Accessed: 22 September 2018).

Palmer, D. (2017b) *Your forgotten IoT gadgets will leave a disastrous, toxic legacy.* Available at: https://www.zdnet.com/article/your-forgotten-IoT-gadgets-will-leave-a-disastrous-toxic-legacy/ (Accessed: 23 September 2018).

Palmer, D. (2018a) *This password-stealing malware uses Facebook Messenger to spread further.* Available at: https://www.zdnet.com/article/this-password-stealing-malware-uses-facebook-messenger-to-spread-further/ (Accessed: 11 September 2018).

Palmer, D.(2018b) *Telegram Zero-Day let hackers spread backdoor and cryptocurrency-mining malware.*. Available at: https://www.zdnet.com/article/

telegram-zero-day-let-hackers-spread-backdoor-and-cryptocurrency-mining-malware/ (Accessed 24 March 2020).

Palmer, D. (2020a) *Cybersecurity warning: 10 ways hackers are using automation to boost their attacks*. Available at: https://www.zdnet.com/article/cybersecurity-warning-10-ways-hackers-are-using-automation-to-boost-their-attacks/ (Accessed 24 May 2020).

Palmer, D. (2020b) *Warning over "hidden apps" as mobile malware attacks increase - and get sneakier*. Available at: https://www.zdnet.com/article/warning-over-hidden-apps-as-mobile-malware-attacks-increase-and-get-sneakier/ (Accessed 6 May 2020).

Pariser, E. (2011) *The filter bubble: What the internet is hiding from you*. London: Penguin.

Park, E., Kim, K.J. and Ohm, J.Y. (2014) 'Does panel type affect haptic experience? An empirical comparison of touch screen panels for smartphones', *Journal on Multimodal User Interfaces*, 8(4), pp. 429–433. doi: 10.1007/s12193-014-0167-y.

Park, K. and Pak, J. (2012) 'An integrated gateway for various PHDs in u-healthcare environments', *Journal of Biomedicine and Biotechnology*, 2012, pp. 1–7. doi: 10.1155/2012/954603.

Paullet, K. and Pinchot, J. (2014) 'Mobile malware: Coming to a smartphone near you?', *Issues in Information Systems*, 15(2), pp. 116–123.

PC Tools (2016) *What is a Zero-Day vulnerability?* Available at: http://www.pctools.com/security-news/zero-day-vulnerability/ (Accessed: 7 December 2016).

Perekalin, A. (2019) 'How Pirates Hook Gamers', *Kaspersky Daily,* 15 February. Available at: https://www.kaspersky.co.uk/blog/how-pirates-hook-gamers/15360/ (Accessed: 20 July 2020).

Perera, C., Liu, C.H. and Jayawardena, S. (2015) *IEEE Transactions on emerging topics in computing: The emerging Internet of Things marketplace from an industrial perspective: A survey*. Available at: https://arxiv.org/PDF/1502.00134.PDF (Accessed: 14 February 2017).

Perez, S. (2016) *Nearly 1 in 4 people abandon mobile apps after only one use* Available at: https://techcrunch.com/2016/05/31/nearly-1-in-4-people-abandon-mobile-apps-after-only-one-us (Accessed: 21 December 2019).

Pizarro, J., Corsaro, N. and Yu, S. (2007) 'Journey to crime and victimization: An application of routine activities theory and environmental criminology to homicide', *Victims and Offenders*, 2(4), pp.375-394.

Plummer, D.C., Baker, V.L., Austin, T., Smulders, C., Tully, J., Valdes, R., Sarner, A., Moyer, K.R., Karamouzis, F., Andrews, W., Heiser, J., Fabre, S., McIntyre, A., Scheibenreif, D., Hobert, K.A., Sussin, J., Marshall, R., Smith, R., Kihn, M., Revang, M., Leow, A., Wong, J., Morello, D., Furlonger, D., Brant, K.F. and Poitevin, H. (2015) *Top strategic predictions for 2016 and beyond: The future is a digital thing*. Available at: https://www.gartner.com/doc/3142020?ref=unauthreader (Accessed: 5 September 2016).

Poletti, A. and Rak, J. (2013) *Identity technologies: Constructing the self, online,* Wisconsin. The University of Wisconsin Press.

Pollette, C. and Crawford, S. (2020) *What is an IP address?* Available at: https://computer.howstuffworks.com/internet/basics/what-is-an-ip-address.html. (Accessed: 9 June 2020).

Polly, J. A. (1992) *Surfing the internet : An introduction, version 2.0.2*. Champaign, IL: Project Gutenberg. Available at: http://search.ebscohost.com.ezproxy.derby.ac.uk/login.aspx?direct=true&db=nlebk&AN=1085446&site=eds-live (Accessed: 17 June 2020).

Ponemon Institute (2019) *The third annual study on third party IoT risk: Companies don't know what they don't know: The Shared Assessments Program.* Available at: https://sharedassessments.org/2019-IoTstudy/ (Accessed: 8 February 2020).

Pori Khabar (2018) *10 most unusual and weird mobile apps you must know about.* Available at: https://poorikhabar.com/2018/06/01/10-most-unusual-and-weird-apps-you-must-know-about/ (Accessed: 12 December 2019).

Porup, J.M. (2019) *What is a zero day? A powerful but fragile weapon*. Available at: https://www.csoonline.com/article/3284084/what-is-a-zero-day-a-powerful-but-fragile-weapon.html (Accessed 9 June 2020)

Popyack, J. (2008) *Computers, basic functionalities, and computing devices: Examples of devices with embedded computers.* Available at:

https://www.cs.drexel.edu/~introcs/Fa08/notes/02.2_ComputingDevices/examples.html?CurrentSlide=5 (Accessed: 7 July 2017).

Poremba, S.M. (2018) *How a VPN can boost your security and privacy.* Available at: https://www.tomsguide.com/uk/us/-vpn-for-beginners,news-17514.html?region-switch=1589747437 (Accessed: 18 May 2020).

Portable Apps (2016) *Safe portable app-ing. Portable software for USB, portable and cloud drives*. Available at: http://portableapps.com/support/safe _portable_ app-ing (Accessed: 1 December 2016).

Potchak, M., McGloin, J. and Zgoba, K. (2002) 'A spatial analysis of criminal effort: Auto theft in Newark, New Jersey', *Criminal Justice Policy Review*, 13(3), pp.257-285.

Pratt, M. (2019) *Kodi Boxes: Everything you need to know.* Available at: https://www.which.co.uk/reviews/internet-tv-boxes/article/kodi-boxes-everything-you-need-to-know (Accessed: 7 November 2019).

Prensky, M. (2001) 'Digital natives, digital immigrants part 1', *On the Horizon*, 9(5), pp.1-6.

Proofpoint (2015) 'Is Nothing Sacred? Risky Mobile Apps Steal Data and Spy On Users', *Proofpoint*, 16 December. Available at: https://www.proofpoint.com/us/threat -insight/post/Risky-Mobile-Apps-Steal-Data (Accessed: 19 March 2020).

Przybylski, A.K., Murayama, K. DeHaan, C.R. and Gladwell, V. (2013) 'Motivational, emotional, and behavioural correlates of fear of missing out', *Computers in Human Behavior* 29 (4), 1841–48. doi:10.1016/j.chb.2013.02.014.

Ptsecurity (2017) *Attacks on corporate Wi-Fi networks*. Available at: https://www.ptsecurity.com/ww-en/analytics/attacks-on-corporate-wi-fi-networks/ (Accessed:20 February 2020).

Puranik, M.(2019) *Bluetooth hacks keep evolving, will your cybersecurity strategy?* Available at: www.infosecurity-magazine.com/opinions/bluetooth-hacks-strategy/(Accessed: 18 June 2020).

Putman, P. (2019) 'The consequences of digital piracy', *United States Cybersecurity Magazine*. Available at: https://www.uscybersecurity.net/digital-piracy/ (Accessed: 11 November 2019).

PwC (2013) *Millennials at work reshaping the workplace*. Available at: https://www.pwc.com/m1/en/services/consulting/documents/millennials-at-work.PDF (Accessed: 25 November 2016).

PwC (2018) *Global economic crime survey.* Available at https://www.pwc.co.uk/services/forensic-services/insights/global-economic-crime-survey-2018---uk-findings.html (Accessed: 22 August 2018).

Punithavathani, D.S., Sujatha, K. and Jain, J.M. (2014) 'Surveillance of anomaly and misuse in critical networks to counter insider threats using computational intelligence', *Cluster Computing*, 18(1), pp. 435–451.

Qamar, A., Karim, A. and Chang, V. (2019) 'Mobile malware attacks: Review, taxonomy and future directions', *Future Generation Computer Systems -The*

International Journal of Escience, 97, pp. 887–909. doi: 10.1016/j.future.2019.03.007.

Qian, C., Luo, X., Le, Y. and Gu, G. (2015) 'VulHunter: Toward discovering vulnerabilities in Android applications', *IEEE Micro*, 35(1), pp. 44–53. doi: 10.1109/mm.2015.25.

Quick, D. and Choo, K. (2016) 'Digital forensic intelligence: data subsets and open source intelligence (DFINT+OSINT): A timely and cohesive mix', *Future Generation Computer Systems*, 78, pp.558-567.

Radoglou Grammatikis, P., Sarigiannidis, P. and Moscholios, I. (2019) 'Securing the Internet of Things: Challenges, threats and solutions', *Internet of Things*, 5, pp.41-70.

Raghuramu, A., Pathak, P.H., Zang, H., Han, J., Liu, C. and Chuah, C.-N. (2016) 'Uncovering the footprints of malicious traffic in wireless/mobile networks', *Computer Communications,* 95, pp. 95–107. doi: 10.1016/j.comcom.2016.04.011.

Ramakrishnan, U. P. and Tandon, J. K. (2018) 'The evolving landscape of cyber threats', *Vidwat: The Indian Journal of Management*, 11, pp. 31–35. Available at: https://search-ebscohost-com.ezproxy.derby.ac.uk/login.aspx? direct=true&db= bth&AN=139235797&site=eds-live (Accessed: 12 August 2020).

Ramsey, R. (2019) *Guide to tagging on social media*. Available at: https://www.theukdomain.uk/tagging-on-social-media/ (Accessed: 20 May 2020).

Razak, M.F.A., Anuar, N.B., Salleh, R. and Firdaus, A. (2016) ‘The rise of “malware”: Bibliometric analysis of malware study’, *Journal of Network and Computer Applications*, 75, pp. 58–76. doi: 10.1016/j.jnca.2016.08.022.

Reinhard, P. (2016) ‘Readers’ Comments’, *Gadgets’,* 21 July. Available at: https://gadgets.ndtv.com/apps/features/how-to-turn-off-automatic-app-updates-in-android-ios-windows-phone-81-windows-81-634685 (Accessed: 28 October 2019).

Reis, C., Barth, A. and Pizano, C. (2009) ‘Browser security: Lessons from Google Chrome’, *Queue*, 7(5), p. 3. doi: 10.1145/1551644.1556050.

Reynald, D. M. (2009) ‘Guardianship in action: Developing a new tool for measurement’. *Crime Prevention and Community Safety*, 11(1), pp.1-20.

Reynald, D. M. (2010) ‘Guardians on guardianship: Factors affecting the willingness to supervise, the ability to detect potential offenders, and the willingness to intervene. *Journal of Research in Crime and Delinquency*, 47(3), pp.358–390.

Ring, T. (2015) ‘The enemy within’, *Computer Fraud and Security*, 2015(12), pp. 9–14. doi: 10.1016/s1361-3723(15)30111-1.

Rivera, D., George, G., Peter, P., Muralidharan, S. and Khanum, S. (2013) *Analysis of security controls for BYOD (bring your own device)*. Available at: http://hdl.handle.net/11343/33338 (Accessed: 2 July 2016).

Rizzo, B. (2016) ‘Data of 200 million Yahoo users for sale on the dark web’, *Database and Network Journal*, p.13. *Expanded Academic ASAP*,

go.galegroup.com/ps/i.do?p=EAIM&sw=w&u=derby&v=2.1&id=GALE%7CA46144
4810&it=r&asid=9e91a85834c0532a086754fc4271f662. (Accessed: 7 February
2017).

Roberts, L. D. (2015) ‘Ethical issues in conducting qualitative research in online communities’, *Qualitative Research in Psychology*, 12(3), pp. 314–325. Doi: 10.1080/14780887.2015.1008909.

Ross, A. (2018) *Building an effective cyber defence against polymorphic malware*. Available at: https://www.information-age.com/building-an-effective-cyber-defence-against-polymorphic-malware-123474759/ (Accessed: 21 September 2018).

Rosser, M. (2017) *Getting started with hashtags on LinkedIn*. Available at: https://www.linkedin.com/pulse/getting-started-hashtags-linkedin-mindi-rosser (Accessed: 26 March 2018).

Rossi, B. (2015) *Don’t allow your guest Wi-Fi to become a security risk.* Available at: https://www.information-age.com/dont-allow-your-guest-wi-fi-become-security-risk-123460490/ (Accessed: 22 December 2019).

Roth, I. (2016) *Smart sensors at the forefront of building intelligence: Smart buildings*. Available at: http://www.smartbuildingsmagazine.com/features/smart-sensors-at-the-forefront-of-building-intelligence (Accessed: 5 October 2016).

Roth, J. and Roberts, J. (2015) ‘Now, later, or not at all: Personal and situational factors impacting burglars’ target choices’, *Journal of Crime and Justice*, 40(2), pp.119-137.

Rouse, M. (2020) *Encryption*. Available at: https://searchsecurity.techtarget.com/definition/encryption (Accessed: 6 July 2020).

Rouse, M. and Burke, J. (2020) *What is VPN (virtual private network)?* Available at: https://searchnetworking.techtarget.com/definition/virtual-private-network (Accessed: 18 May 2020).

Rouse, M. and Haughn, M. (2019) *What is attack surface? - Definition from WhatIs.com*. Available at: https://whatis.techtarget.com/definition/attack-surface (Accessed: 21 June 2019)

Ruan, X., Wu, Z., Wang, H. and Jajodia, S. (2016) 'Profiling online social behaviours for compromised account detection', *IEEE Transaction on Information Forensics and Security*, 11(1), pp. 176–187. doi: 10.1109/tifs.2015.2482465.

Rughiniş, C. and Rughiniş, R. (2014) 'Nothing ventured, nothing gained. Profiles of online activity, cybercrime exposure, and security measures of end-users in European Union', *Computers and Security*, 43, pp.111-125.

Russell, C. (2016) 'Assessing the risk of transformative technologies', *Computer Fraud and Security*, 27, pp.15–19. doi: 10.1016/s1361-3723(16)30054-9.

Ryan, L. (2015) 'Readers Comments', *Gadgets,* 30 November. Available at: https://gadgets.ndtv.com/apps/features/how-to-turn-off-automatic-app-updates-in-android-ios-windows-phone-81-windows-81-634685 (Accessed: 28 October 2019).

Safa, N.S., Maple, C., Furnell, S., Azad, M.A., Perera, C., Dabbagh, M. and Sookhak, M. (2019) 'Deterrence and prevention-based model to mitigate

information security insider threats in organisations', *Future Generation Computer Systems*, 97, pp. 587–597. doi: 10.1016/j.future.2019.03.024.

Safaei Pour, M., Bou-Harb, E., Varma, K., Neshenko, N., Pados, D. and Choo, K. (2019) 'Comprehending the IoT cyber threat landscape: A data dimensionality reduction technique to infer and characterize Internet-scale IoT probing campaigns', *Digital Investigation*, 28, pp. S40-S49.

Safruti, I. (2020) 'PerimeterX Researcher Finds Vulnerability in WhatsApp Desktop Platform', *PerimeterX* , 4 February. Available at: https://www.perimeterx .com/ resources/blog/2020/perimeterx-researcher-finds-vulnerability-in-whatsapp/ (Accessed: 6 April 2020).

Salim, H.M. and Madnick, S.E. (2014) *Cyber safety: A systems thinking and systems theory approach to managing cyber security risks*. Available at: http://ic3.mit.edu/ResearchSamples/2014-12.PDF (Accessed: 3 October 2016).

Sampson, R., Eck, J. and Dunham, J. (2009) 'Super controllers and crime prevention: A routine activity explanation of crime prevention success and failure'. *Security Journal*, 23(1), pp.37-51.

Sarma, S. (2015) *I helped invent the Internet of things. Here's why I'm worried about how secure it is*. Available at: http://www.politico.com/agenda/story /2015/06/internet-of-things-privacy-risks-security-000096 (Accessed: 16 February 2017).

Sarson, (2020)' Social media statistics in the UK', *Talkwalker'*, 5 February. Available at: https://www.talkwalker.com/blog/social-media-statistics-in-the-uk (Accessed: 20 June 2020).

Saxena, N., Hayes, E., Bertino, E., Ojo, P., Choo, K.-K.R. and Burnap, P. (20N0) ‘Impact and key challenges of insider threats on organizations and critical businesses’, *Electronics (Basel)*, 9, (9). doi:10.3390/electronics9091460

Scott, D. (2016) *ISTR insights: The Internet of Things (IoT) and the concerns of convenience*. Available at: https://www.symantec.com/connect//istr-insights-the-internet-of-things-IoT-and-the-concerns-of-convenience (Accessed: 14 February 2017).

Scroxton, A. (2020) *Malicious apps still getting past Google controls.* Available at: https://www.computerweekly.com/news/252478952/Malicious-apps-still-getting-past-Google-controls (Accessed 6 May 2020).

Seals, T. (2020) *Apple iPhone users targeted with bogus dating app for Valentine’s Day*. Available at: https://threatpost.com/apple-iphone-dating-app-valentines-day/152911/ (Accessed 6 May 2020).

Seebruck, R. (2015) ‘A typology of hackers: Classifying cyber malfeasance using a weighted arc circumplex model’, *Digital Investigation*, 14, pp. 36–45. doi: 10.1016/j.diin.2015.07.002.

Sensoria (2014) *Sensoria smart socks – a better way to run.* https://www.sensoriafitness.com/ (Accessed 25 March 2020).

SentinelOne (2016) *In today’s cyber threat landscape, not all attacks are created equal.* Available at: https://www.sentinelone.com/wp-content/uploads/2016/05/MalwareVsExploit_WP_051116.PDF (Accessed: 20 January 2017).

Setterstrom, A.J., Pearson, J.M. and Orwig, R.A. (2013) ‘Web-enabled wireless technology: An exploratory study of adoption and continued use intentions’, *Behaviour and Information Technology*, 32(11), pp. 1139–1154.

Seyler, D., Li,L.and Zhai,C. (2020) *Identifying compromised accounts on social media using statistical text analysis.* Available at: https://arxiv.org/pdf/1 804.07247 (Accessed:23 June 2020).

Shabtai, A., Tenenboim-Chekina, L., Mimran, D., Rokach, L., Shapira, B. and Elovici, Y. (2014) ‘Mobile malware detection through analysis of deviations in application network behaviour’, *Computers and Security*, 43, pp. 1–18.

Shaikh, A. and Oliveira, D. (2019) ‘Informal IT and routine activity theory - a theoretical review’, *SoutheastCon,* pp. 1- 4. doi: 10.1109/SoutheastCon 42311.2019.9020557.

Shaikh, S. (2019) *Why mobile apps require access to your data and device tools*. Available at: https://economictimes.indiatimes.com/small-biz/security-tech/technology/why-mobile-apps-require-access-to-your-dataand-device-tools/articleshow/52138161.cms (Accessed: 12 February 2020).

Shillito, M. R. (2019) ‘Untangling the “dark web”: An emerging technological challenge for the criminal law’, *Information and Communications Technology Law*, 28(2), pp. 186–207. doi: 10.1080/13600834.2019.1623449.

Siboni, S., Shabtai, A., Tippenhauer, N.O., Lee, J. and Elovici, Y. (2016) ‘Advanced security testbed framework for wearable IoT devices’, *ACM Transactions on Internet Technology*, 16(4), pp. 1–25..

Silic, M. and Back, A. (2014) ‘Shadow IT: A view from behind the curtain’, *Computers and Security*, 45, pp. 274–283.

Silic, M. and Back, A. (2016) ‘The dark side of social networking sites: Understanding phishing risks’, *Computers in Human Behavior*, 60, pp. 35–43.

Similarweb (2020) *Xvideos.* Available at: https://www.similarweb.com/website/xvideos.com (Accessed: 24 March 2020).

Simonite, T. (2016) *Machine-learning algorithms make for great cybercriminals.* MIT Technology Review. Available at: https://www.technologyreview.com/s/602109/this-ai-will-craft-tweets-that-youll-never-know-are-spam/ (Accessed: 24 August 2018).

Singh, M. (2020) *WhatsApp hits 2 billion users, up from 1.5 billion 2 years ago*. Available at: https://techcrunch.com/2020/02/12/whatsapp-hits-2-billion-users-up-from-1-5-billion-2-years-ago/? (Accessed, 27 June 2020).

Singh, U.K., Joshi, C. and Kanellopoulos, D. (2019) ‘A framework for zero-day vulnerabilities detection and prioritization’, *Journal of Information Security and Applications*, 46, pp.164–172.

Sinicki, A. (2019) *Root Android: Everything you need to know.* Available at: https://www.androidauthority.com/root-android-277350/ (Accessed 20 June 2020).

Sjöberg, L. and Fromm, J. (2001) ‘Information technology risks as seen by the public’, *Risk Analysis*, 21(3), pp. 427–442. doi: 10.1111/0272-4332.213123.

Skyhigh (2016) C*loud adoption risk report*. Available at: http://info.skyhighnetworks.com/ rs/274-AUP-214/images/WP-Cloud-Adoption-and-Risk-Report-Q4-2016.PDF (Accessed: 31 January 2017).

Slattery, D. (2018) *How to keep your guest WiFi free from cyber- attacks.* Available at: https://insidesmallbusiness.com.au/planning-management/how-to-keep-your-guest-wifi-free-from-cyber-attacks (Accessed:20 February 2020).

Smartmat (2018 *) It's like having your own personal yoga teacher.* Available at https://smartmat.com (Accessed 25 March 2020).

Smejkal, I. (2017) *Digital Footprints: how social media can affect your job prospects.* Available at: http://www.sandersonplc.com /news/digital-footprints-how-social-media-can-affect-your-job-prospects (Accessed: 22 August 2018).

Snelling, D. (2019) *Netflix and Sky TV dominance can't stop millions streaming illegally*. Available at: https://www.express.co.uk/life-style/science-technology/1189534/Sky-TV-Netflix-illegal-streaming-movies-TV-sports (Accessed: 7 November 2019).

Snyder, J. (2019) *What are the security risks of rooting your smartphone?* Available at: https://insights.samsung.com/2019/05/29/what-are-the-security-risks-of-rooting-your-smartphone/(Accessed 25 July 2020).

Smart Survey (2019) *Adding a save and continue later option*. Available from: https://help.smartsurvey.co.uk/article/adding-a-save-and-continue-later-option (Accessed: 11 June 2019).

Smith, C. (2019) *Home devices you can control with your smartphone*. Available at: https://home.bt.com/tech-gadgets/internet/connected-home/lights-camera-kitchen-9-ways-to-control-your-home-from-your-smartphone-11364005104661 (Accessed: 8 February 2020).

Smith, N. (2013) *Using the Internet as an Intelligence Tool.* UK OSINT Training Course [London. 20-23 January]

Smith, N. (2014) *Using Social Networks to Identify Suspects*. UK OSINT Training Course [Leicester.13 November]

Solomon, B, and Fox-Brewster, T (2016) 'Hacked cameras were behind today's massive web outage', *Forbes.Com*, p. 6, Business Source Premier, EBSCO*host*, (Accessed: 6 February 2017).

Sood, A. and Enbody, R. (2011) 'Chain exploitation—social networks malware', *ISACA Journal*, 1, pp.31-36. Available at: http://www.isacajournal-digital.org/isacajournal/2011vol1#pg33 (Accessed: 23 September 2018).

Spapens, T. (2010) 'Macro networks, collectives, and business processes: An integrated approach to organized crime', *European Journal of Crime, Criminal Law and Criminal Justice* 18(2), 185-216.

Spiezle, C. (2016) Statement for the record. "Understanding the role of connected devices in recent Cyber-attacks". United States House of Representatives Committee on Energy and Commerce'. Available at: http://totalliance.acton software.com/acton/attachment/6361/f-009d/1/-/-/-/-/House%20Statement%2011-15.PDFIoT (Accessed: 18 November 2016).

Stahl, B.C. (2013) ‘Interpretive accounts and fairy tales: a critical polemic against the empiricist bias in interpretive IS research’, *European Journal of Information Systems* (1) Pp1-11.

Stanojevic, M. (2020) The 5 best firewall devices to protect your home network. Available at: https://windowsreport.com/firewall-device-for-home/ (Accessed: 18 May 2020).

Statista (2019) *Percentage of all global web pages served to mobile phones from 2009 to 2018.* Available at: https://www.statista.com/statistics/241462/global-mobile-phone-website-traffic-share/ (Accessed: 6 May 2020).

Statista (2020a) *Number of smartphone users worldwide from 2016 to 2021.* Available at: https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/ (Accessed: 11 June 2020).

Statista (2020b) *Global social media statistics.* Available at: https://www.statista.com/opics/1164/social-networks/ (Accessed: 21 June 2020)

Statista (2020c) *IoT: Number of connected devices worldwide 2012-2025* Available at: https://www.statista.com/statistics/471264/IoT-number-of-connected-devices-worldwide/ (Accessed: 3 February 2020).

Statista (2020d) *Mobile games - United Kingdom, Statista market forecast.* Available at: https://www.statista.com/outlook/211/156/mobile-games/united-kingdom?currency=gbp#market-arpu (Accessed: 17 March 2020).

Stegner, B. (2016) *7 best tools to tweak and customize Windows 10*. Available at: http://www.makeuseof.com/tag/7-best-tools-tweak-customize-windows-10/ (Accessed: 1 December 2016).

Stojanovic, B. (2011) 'The consequences of the unpredictable and the unexpected. The Black Swan - the impact of the highly improbable by Nassim Nicholas Taleb', *Panoeconomicus*, 58(2), pp. 277–284.

Stokel-Walker, C. (2019) *To compete with Netflix, online piracy is upping its game*. Available at: https://www.wired.co.uk/article/online-video-piracy-is-on-the-rise (Accessed: 12 November 2019).

Storey, A. (2014) 'There's nothing "smart" about insecure connected devices', *Network Security*, 2014(7), pp. 9–12. doi: 10.1016/s1353-4858(14)70069-8.

Stripe, N. (2020) *Crime in England and Wales: Year ending December 2019.* Available at: https://www.ons.gov.uk/peoplepopulationandcommunity/ crimeandjustice /bulletins/crimeinenglandandwales/yearending december2019#computer-misuse (Accessed: 17 May 2020).

Stubbington, T. (2017) 'Cyber-slackers doom UK economy: Apps are addictive, and 'hijack the mind''. *Sunday Times*, (26 November).

Sweeten, G., Sillence, E. and Neave, N. (2018) 'Digital hoarding behaviours: Underlying motivations and potential negative consequences', *Computers in Human Behavior*, 85, pp.54-60.

Sweney, M. (2019) *More than half of people aged 65 and over now shop online – ONS*. Available at**:** https://www.theguardian.com/money/2019/aug/12/more-than-half-of-people-aged-65-and-over-now-shop-online-ons (Accessed: 12 June 2020)

Swider, M. (2016) *Google glass review*. Available at: http://www.techradar.com/reviews/gadgets/google-glass-1152283/review (Accessed: 13 February 2017).

Sydow, L. (2018) '2019 in mobile: 5 things you need to know'*, App Annie,* 05 December. Available at: https://www.appannie.com/en/insights/market-data/2019-in-mobile-5-things-to-know/ (Accessed: 30 October 2019).

Sydow, L. and Cheney, S. (2018) *2017 retrospective: a monumental year for the app economy.* Available at: https://www.appannie.com/en/insights/market-data/app-annie-2017-retrospective/ (Accessed: 31 March 2020).

Symantec (2015) *Internet security threat report: Volume 20.* Available at: https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347932_GA-internet-security-threat-report-volume-20-2015-social_v2.PDF (Accessed: 14 January 2016).

Symantec (2016) *Internet security threat report: Volume 21*. Available at: https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.PDF?aid=elq_&om_sem_kw=elq_16287733&om_ext_cid=biz_email_elq_&elqTrackId=283a3acdb3ff42f4a70ab5a9f236eb71&elqaid=2902&elqat=2 (Accessed: 20 July 2016).

Symantec (2017) *Internet security threat report: Volume 22.* Available at: https://resource.elq.symantec.com/e/f2 (Accessed: 11 January 2018).

Symantec (2018) *Internet security threat report: Volume 23.* Available at: https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.PDF. (Accessed: June 2018).

Symantec (2019) *Internet security threat report: Volume 24.* Available at: https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.PDF. (Accessed: June 2019).

Mckinsey Quarterly (2009) 'Taking improbable events seriously: An interview with the author of The Black Swan', (2009) *Mckinsey Quarterly*, 1, pp. 47-49, Business Source Premier, EBSCO *host*, (viewed: 14 February 2017).

Taleb, N. N. (2007) *The Black Swan: The impact of the highly improbable.* New York: Random House.

Tanasychuk, M. (2016) *Best cloud storage apps for iPhone and iPad*. Available at: http://www.imore.com/best-cloud-storage-apps-iphone-ipad (Accessed: 31 January 2017).

Taranowicz, I. (2018) ‘New technologies and institutionalization of everyday family life in liquid modernity’, *Studia Humanistyczne AGH*, 17(4), pp. 69–76. doi: 10.7494/human.2018.17.4.69.

Tarquin. (2016) *How to access the dark web | dark web news*. Available at: https://darkwebnews.com/help-advice/access-dark-web/ (Accessed: 8 Jul. 2017).

Techopedia Securities Institute (2017) *What is a Zero-Day threat? - definition from Techopedia*. Available at: https://www.techopedia.com/definition/27451/zero-day-threat (Accessed: 26 January 2017).

Tattersall, S. (2018) *How to build custom IoT hardware with Arduino*. Available at: https://opensource.com/article/17/12/how-build-custom-IoT-hardware-arduino (Accessed: 22 February 2020).

Techopedia (2019) *What is video streaming? - Definition from Techopedia*. Available at: https://www.techopedia.com/definition/9927/video-streaming (Accessed: 31 October 2019).

Techopedia (2020) *Zero-Day Malware.* Available at: https://www.techopedia.com/definition/29741/zero-day-malware (Accessed 23 July 2020).

TechTarget (2002) *How does antivirus software work?* Available at: https://searchsecurity.techtarget.com/answer/How-does-antivirus-software-work (Accessed: 7 September 2018).

TechTarget (2005) *Blended threat*. Available at https://searchsecurity.techtarget.com/definition/blended-threat. (Accessed 14 April 2017).

Techterms (2014) *Digital footprint definition*. Available at: https://techterms.com/definition/digital_footprint (Accessed: 15 August 2018).

Temizkan, O., Kumar, R., Park, S. and Subramaniam, C. (2012) 'Patch release behaviors of software vendors in response to vulnerabilities: An empirical analysis', *Journal of Management Information Systems*, 28(4), pp.305-338.

Tewksbury, R. and Mustaine, E. (2003) 'College students' lifestyles and self-protective behaviours, C*riminal Justice and Behaviour*, 30(3), pp.302-327.

The Associated Press (2019) ‘ASUS acknowledges computers infected by auto-update virus’, *Long Island business news (Ronkonkoma, NY)*. Available at: http://search.ebscohost.com.ezproxy.derby.ac.uk/login.aspx?direct=true&db=bwh&AN=L54115856LIBN&site=eds-live (Accessed:23 March 2020).

The City UK (2017) *UK-based financial and related professional services: Enabling growth across the UK*. Available at: https://www.thecityuk.com/news/cities-across-uk-host-vital-financial-and-related-professional-services-hubs/ (Accessed: 21 July 2017).

The Internet Society (2019) *The trust opportunity: Exploring consumer’s attitudes to the Internet of Things*. Available at: https://www.internetsociety.org/resources/doc/2019/trust-opportunity-exploring-consumer-attitudes-to-IoT/ (Accessed 20 April 2020).

The iPhonewiki (2015) *Jailbreak exploits.* Available at: https://www.com/wiki/Jailbreak_Exploits#Pangu8_.288.0_.2F_8.0.1_.2F_8.0.2_.2F_8.1.29 (Accessed: 4 February 2017).

The Next Wave (2016) ‘When your refrigerator steals your identity’, *The National Security Agencies’ Review of Emerging Technologies*. Available at: https://www.nsa.gov/resources/everyone/digital-media-center/publications/the-next-wave/assets/files/TNW-21-2.PDF (Accessed: 14 February 2017).

The Royal Society (2019a) *iHuman: blurring lines between mind and machine* Available at: http:// www. royalsociety.org/ihuman-perspective (Accessed: 24 May 2020).

The Royal Society (2019b) *Protecting privacy in practice. The current use, development and limits of privacy enhancing technologies in data analysis.* Available at: https://royalsociety.org/-/media/policy/projects/privacy-enhancing-technologies/privacy-enhancing-technologies-report.pdf (Accessed: 24 June 2021).

The Telegraph (2012) *More high street shops to close as shoppers move online*. Available at: http://www.telegraph.co.uk/finance/newsbysector/retailandconsumer/9157237/More-High-Street-shops-to-close-as-shoppers-move-online.html (Accessed: 9 February 2017).

The Tor Project (2018) *Tor Project: Overview*. Available at: https://www.torproject.org/about/overview.html.en (Accessed: 21 March 2018).

The Tor Project (2020*) Tor Project: History*. Available at: https://www.torproject org/about/history/ (Accessed: 8 June 2020).

Thibeault, J. (2018) 'The Elephant in the Live-Streaming Room', *Streaming Media*, 15(8), p.10. Available at: http://search.ebscohost.com.ezproxy.derby.ac.uk/login.aspx?direct=true&db=bth&AN=133220924&site=eds-live (Accessed: 8 November 2019).

Thomas, K. (2004) 'The research process as a journey'. From positivist traditions into the realms of qualitative inquiry' in Goodson, L. and Phillimore, J. (eds) *Qualitative research in tourism: ontologies, epistemologies and methodologies*. Taylor and Francis Group.

Thornton-Trump, I. (2018) 'Malicious attacks and actors: An examination of

the modern cybercriminal' *Edpacs*, 57:1, 17-23, DOI: 10.1080/07366981.2018.1432180

Thrive Networks (2011) *How hackers use backdoors to access a network.* Available at: http://www.thrivenetworks.com/blog/2011/09/22/how-hackers-use-backdoors-to-access-a-network/ (Accessed: 8 July 2017).

Thomas, K. and Nicol, D.M. (2010) 'The Koobface botnet and the rise of social malware', Conference Paper. Institute of Electrical and Electronics Engineers (IEEE).

Thurrott, P. (2019) *Report: smart speaker sales hit a record 86 million units in q4 2018. A*vailable at: https://www.thurrott.com/smart-home/199836/report-smart-speaker-sales-hit-a-record-86-million-units-in-q4-2018 (Accessed: 8 February 2020).

Tilley, N. (2009) *Crime Prevention*, Willan Publishing. Available at https://ebookcentral.proquest.com/lib/derby/detail.action?docID=1924403 (Downloaded: 09 July 2018).

Titcomb, J. (2016) *Internet of Things struggles as use of smart home gadgets flatlines*. Available at: http://www.telegraph.co.uk/technology/2016/08/27/internet-of-things-struggles-as-use-of-smart-home-gadgets-flatli/ (Accessed: 16 February 2017).

Tomazic, T. and Vilela, N. (2017) 'Ongoing criminal activities in cyberspace: from the protection of minors to the deep web', *Ravia za Kriminalistiko In Kriminologijo*, 68.

Tran, H., Campos-Nanez, E., Fomin, P. and Wasek, J. (2016) ‘Cyber resilience recovery model to combat zero-day malware attacks’, *Computers and Security*, 61, pp. 19–31. doi: 10.1016/j.cose.2016.05.001.

Treanor, J. and Collinson, P. (2017) *HSBC to close 62 more branches this year, blaming online banking*. Available at: https://www.theguardian.com/business /2017/jan/24/hsbc-close-branches-online-banking-unions-jobs (Accessed: 9 February 2017).

TrendMicro (2020) *Exploit kit.* Available at: https://www.trendmicro.com/vinfo/us/security/definition/exploit-kit (Accessed:12 July 2020).

Tsai, H.S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N.J. and Cotten, S.R. (2016) ‘Understanding online safety behaviours: A protection motivation theory perspective’, *Computers and Security*, 59, pp. 138–150.

Tsikerdekis, M. and Zeadally, S. (2014) ‘Online deception in social media’, *Communications of the ACM*, 57(9), pp. 72–80. doi: 10.1145/2629612.

Tweneboah-Koduah, S., Skouby, K. and Tadayoni, R. (2017) ‘Cyber Security Threats to IoT Applications and Service Domains’, *Wireless Personal Communications*, 95(1), pp.169-185.

Twitter Inc (2017) *Using hashtags on Twitter*. Available at: https://support.twitter.com/articles/49309# (Accessed: 25 November 2017).

Tyler, J. (2016) ‘Don’t be your own worst enemy: protecting your organisation from inside threats’ *Computer Fraud & Security*, 8, pp. 19-20, https://doi.org/10.1016/S1361-3723(16)30063-X.

United States Attorney’s Office (2015) *IT professional sentenced to 15 months in prison for installing and activating malicious code*. Available at: https://www.justice.gov/usao-md/pr/it-professional-sentenced-15-months-prison-installing-and-activating-malicious-code (Accessed: 26 January 2017).

University of Derby (2011) *Research ethics policy and code of conduct.* Available at: ttps://studylib.net/doc/7745445/university-of-derby-research-ethics-policy-and-code-of-conduct (Accessed: 13 May 2020).

Utter, C.J., Rea, A. (2015) ‘The "bring your own device" conundrum for organisations and investigators: An examination of the policy and legal concerns in light of investigatory challenges’, *The Journal of Digital Forensics, Security and Law* 10(2), Pp. 55-71.

Varsanov, E. (2016) *KoobFace worm virus removal*. Available at: http://www.virusresearch.org/koobface-worm-virus-removal/ (Accessed: 9 February 2017).

Veracode (2016) *How do vulnerabilities get into software? WhitePaper*. Available at http://www.veracode.com/sites/default/files/Resources/Whitepapers/how-vulnerabilities-get-into-software-veracode.PDF (Accessed: 26 January 2017).

Verizon (2015) *RP data breach investigation report 2015*. Available at: http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigation-report_2015_en_xg.PDF (Accessed: 3 July 2016).

Verizon (2020) *Data breach investigations report.* Available at: https://enterprise.verizon.com/resources/reports/dbir/ (Accessed 10 June 2020)

Vermesan, O. and Friess, P. (2014) *Internet of Things – from research and innovation to market deployment.* Available at: http://www.internet-of-things-research.eu/PDF/IoT-From%20Research%20and%20Innovation%20to%20Market%20Deployment_I ERC_Cluster_eBook978-87- 93102_ -95-8_P.PDF (Accessed: 3 July 2016).

Vincent, J. (2019) *Kohler's smart toilet promises a 'fully-immersive experience'.* Available at: https://www.theverge.com/2019/1/6/18170575/kohler-konnect-bathroom-smart-gadgets-numi-intelligent-toilet-ces-2019 (Accessed: 3 February 2020).

VisaEurope (2018) *The contactless revolution ten years on*. Available at: https://www.visaeurope.com/newsroom/news/the-contactless-revolution-ten-years-on (Accessed: 2 September 2018).

Vishwanath, A. (2015) 'Habitual Facebook use and its impact on getting deceived on social media', *Journal of Computer-Mediated Communication*, 20(1), pp. 83–98. doi: 10.1111/jcc4.12100.

Viswanathan, P. (2019) *What makes Apple so special?* Available at: https://www.lifewire.com/what-makes-apple-so-special-and-desirable-2373223 (Accessed: 6 March 2020).

Vyas, S., Shukla, V. and Doshi, N. (2019) ‘FMD and Mastitis disease detection in cows using Internet of Things (IOT)’, *Procedia Computer Science*, 160, pp.728-733.

W3C (2008) *Web content accessibility guidelines (WCAG) 2.0*. Available at: http://www.w3.org/TR/WCAG20/ (Accessed: 25 November 2016).

Wagenseil, P. (2013) *Dropbox used by Chinese hackers to spread malware*. Available at: http://www.nbcnews.com/technology/dropbox-used-chinese-hackers-spread-malware-6C10642402 (Accessed: 8 February 2017).

Walker-Osborn, C., Mann, S. and Mann, V. (2013) 'To BYOD or … not to BYOD’, *ITNow*, 55, 1, p. 38, (Accessed: 2 July 2016).

Wang, D. (2017) ‘A study of the relationship between narcissism, extraversion, drive for entertainment, and narcissistic behaviour on social networking sites’, *Computers in Human Behavior*, 66, pp. 138–148. doi: 10.1016/j.chb.2016.09.036.

Wang, X., Sun, Y., Nanda, S. and Wang, X. (2019) ‘Looking from the mirror: Evaluating IoT device security through mobile companion apps’. *28th USENIX Security Symposium.*

Warkentin, M. and Willison, R. (2009) ‘Behavioural and policy issues in information systems security: The insider threat’, *European Journal of Information Systems*, 18(2), pp. 101–105. doi: 10.1057/ejis.2009.12.

Warman, M. (2020) W*hy the UK is banning default passwords in IoT devices*. Available at: https://tech.newstatesman.com/security/uk-banning-default- (Accessed: 15 February 2020).

Webroot (2019) *Webroot threat report 2019*. Available at: https://www.webroot.com/gb/en/business/threat-intelligence/resources (Accessed: 16 January 2020).

Webroot (2020) *Webroot threat report 2020.* Available at: https://www.webroot.com/gb/en/business/threat-intelligence/resources (Accessed: 4 May 2020).

Wearn, R. (2016) *Banks close more than 600 branches over the past year*. Available at: http://www.bbc.co.uk/news/business-36268324 (Accessed: 9 February 2017).

West, S. (2018) *Everything is online nowadays.* Available at: https://www.ageuk.org.uk/...publications/.../rb_may18_everything_is_online_nowadays (Accessed: 23 August 2018).

Weinberg, B. D., Milne, G. R., Andonova, Y.G., Hajjat, F.M. (2015) 'Internet of Things: Convenience vs. privacy and secrecy', *Business Horizons*, 58 615-624. doi: 10.1016/j.bushor.2015.06.005

Werlinger, R., Hawkey, K. and Beznosov, K. (2009) 'An integrated view of human, organizational, and technological challenges of IT security management', *Information Management and Computer Security*, 17(1), pp. 4–19. doi: 10.1108/09685220910944722.

WhatsApp (2020) *FAQ - protecting our users from a video calling cyber-attack*. Available at: https://faq.whatsapp.com/help/video-calling-cyber-attack (Accessed: 6 April 2020).

Which (2020) *How to spot a messaging scam.* Available at: https://www.which.co.uk/consumer-rights/advice/how-to-spot-a-messaging-scam (Accessed: 5 April 2020).

White, H. (2019) *Voice assistants are taking over consumer IoT.* Available at: https://www.IoTforall.com/voice-assistants-consumer-IoT/ (Accessed: 3 February 2020).

Whittacker, Z. (2018) *New malware pulls its instructions from code hidden in memes posted to Twitter.* Available at: https://techcrunch.com/2018/12/17/malware-commands-code-twitter-hidden-memes/ (Accessed: 3 April 2020).

Whittacker, Z. (2019) *A powerful spyware app now targets iPhone owners.* Available at: https://techcrunch.com/2019/04/08/iphone-spyware-certificate/ (Accessed 6 May 2020).

Whittle, L. (2020) C*ouncil post: Five emerging trends as millennials run manufacturing's next act*. Available at: https://www.forbes.com/sites/forbestechcouncil/2020/01/02/five-emerging-trends-as-millennials-run-manufacturings-next-act/#237064e35869 (Accessed 23 May 2020).

Wikipedia (2020) *List of social networking websites*. Available at: https://en.wikipedia.org/wiki/Listofsocialnetworkingwebsites (Accessed: 1 September 2019).

Wilcox, H. and Bhattacharya, M. (2020) 'A human dimension of hacking: Social engineering through social media', *IOP Conference Series: Materials Science and Engineering*, 790(1). doi: 10.1088/1757-899X/790/1/012040.

Williams, M. and May B.T. (2020). *Best iPhone antivirus apps of 2020.* Available at: https://www.techradar.com/best/best-iphone-antivirus-app (Accessed 6 May 2020).

Williams, P.A.H. (2008) In a 'trusting' environment, everyone is responsible for information security, *Information Security Technical Report*,13(4) pp. 207-215, https://doi.org/10.1016/j.istr.2008.10.009.

Winston, C.E. (2012) 'Biography and life story research', in Laplan, S.D., Quartaroli, M.T. and Riemer, F.J. (eds) *Qualitative research: an introduction to methods and designs***,** Jossey-Bass, San Francisco, California.

Woollaston, V. (2018) *What is Kodi? Everything you NEED to know about the TV streaming app*. Available at: https://www.alphr.com/software/1002235/what-is-kodi-everything-you-need-to-know-about-the-tv-streaming-app (Accessed: 8 November 2019).

Worden, K., Bullough, W.A. and Haywood, J. (2003) *Smart Technologies*. Singapore: World Scientific Publishing

Xbox JailbreakTeam, (2017) *Xbox 360 Jailbreak - how to Jailbreak Xbox 360 with USB*. Available at: http://xboxjailbreak.com/xbox-360-jailbreak/ (Accessed: 4 February 2017).

Xu, Z., Hu, Q. and Zhang, C. (2013) 'Why computer talents become computer hackers', *Communications of the ACM*, 56(4), p. 64. doi: 10.1145/2436256.2436272.

Yablokov, V. (2018) ’Why There’s No Antivirus For iOS’, *Kaspersky,* 10 September. Available at: https://www.kaspersky.co.uk/blog/ios-security-explainer/14425/ (Accessed 6 May 2020).

Yamada, K. (2019)*The best Portable Apps that require no installation*. Available at https://www.makeuseof.com/tag/best-portable-apps/ (Accessed: 6 July 2021).

Yar, M. (2005) The novelty of ‘cybercrime’, *European Journal of Criminology*, 2(4), pp. 407- 427.

Yin, F., Liu, M, and Lin, C. N.D. (2015) 'Forecasting the continuance intention of social networking sites: Assessing privacy risk and usefulness of technology', *Technological Forecasting and Social Change*, 99, pp. 267-272, Social Sciences Citation Index, EBSCO*host*, viewed 25 August 2016.

Yoon, H., Park, S.-H. and Lee, K.-T. (2016) ‘Lightful user interaction on smart wearables’, *Personal and Ubiquitous Computing*, 20(6), pp. 973–984. doi: 10.1007/s00779-016-0959-z.

Yu, M., Zhuge, J., Cao, M., Shi, Z.,. and Jiang, L.(2020) ‘A survey of security vulnerability analysis, discovery, detection, and mitigation on IoT devices’ *Future Internet*, *12* (2) pp. 1-23. doi.org/10.3390/fi12020027.

Zahadat, N., Blessner, P., Blackburn, T. and Olson, B.A. (2015) ‘BYOD security engineering: A framework and its analysis’, *Computers and Security*, 55, pp. 81, 99

ZDNet (2018) *Cyber fraudsters now stealing millions in single transactions.* Available at: https://www.zdnet.com/article/cyber-fraudsters-now-stealing-millions-in-single-transactions/ (Accessed: 23 August 2018).

Zhang, M., Raghunathan, A. and Jha, N.K. (2014) 'A defense framework against malware and vulnerability exploits', *International Journal of Information Security*, 13(5), pp. 439–452. doi: 10.1007/s10207-014-0233-1.

Zheng, Y.L., Ding, X. R., Poon, C.C.Y., Lo, B.P.L., Zhang, H., Zhou, X.L., Yang, G. Z., Zhao, N. and Zhang, Y.T. (2014) 'Unobtrusive sensing and wearable devices for health informatics', *IEEE Transactions on Biomedical Engineering*, 61(5), pp. 1538–1554. doi: 10.1109/tbme.2014.2309951.

Zorz, Z. (2018) *Hacking smart plugs to enter business networks.* Available at: http://www.helpnetsecurity.com/2018/08/23/hacking-smart-plugs/ (Accessed: 23 June 2020).

Zujic, B. (2019) *5 reasons to keep your apps up to date.* Available at: https://www.technobezz.com/5-reasons-keep-apps-date/ (Accessed: 28 Oct. 2019).

Appendix A: Erasing Digital Footprints from the Internet

Introduction

An active footprint remains on the internet indefinitely unless a user is proactive about managing the data available about them. Aside from privacy controls to restrict public access, a user may ask an organisation to delete the data they may be processing. This appendix will briefly summarise the General Data Protection Regulation (GDPR) to inform about erasing data in the context of digital footprints.

The GDPR (2018) was enforced in the UK in May 2018 and affords individuals the 'Right to Erasure', additionally known as 'the Right to be Forgotten' (ICO, 2020a). If specific data protection principles apply, organisations are legally obliged to delete data if requested to do so. Principles ensuring erasure include: the user withdrawing consent, if consent had been a factor in the processing, the processing no longer being necessary, no further legitimate interest in the data, an objection to processing for direct marketing purposes, the data was collected from a child or the data was processed with no 'lawful basis'. Lawful basis is summarised by Gil González and de Hert (2019) as consent, contract, legal obligation, vital interest, public task and legitimate interest.

Under these rules it is possible for users to request that websites delete personal data contributing to a digital footprint, and if the request is upheld, Google will remove websites containing the data from their search results. Consequently, a search for the user's name will no longer return results Google (2020). The right

to erasure is not absolute and exemptions apply which will prevent the data from being removed. These include journalistic, academic, artistic and literary purposes, to abide by legal obligations, public interest or official authority, legal claims, public interest archives or research (ICO, 2020b). In such circumstances a website may refuse to fully comply with the request and the data will remain as a searchable footprint.

Internet search engines can be asked to delete dated information cached (stored) on their servers, to prevent it being returned in search results. In general, a search engine will comply with a removal request, unless the data is additionally stored on pages which are not owned by the search engine, hence it has no control over having it removed (Google, 2018). The Google principle of the 'Right to be Forgotten', entails that when a search is conducted for an individual's name, results will not include links to web pages where the name is referenced. Google will paste a message at the bottom of returned pages to inform that some results have been removed under EU data protection law. This does not mean that the web pages no longer exist, they may still be located using alternative search methods (Arthur, 2014). Changing the default Google setting to Google.com is effective and the practical research documented in Chapters Four and Five used country variants of the Google search engine.

Readers wishing to know more about data protection legislation and the GDPR may be interested in the Information Commissioners Office Guide to Data Protection, an online resource available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-

regulation-gdpr/. To assist users wanting to remove personal data from search results, Google provides an online form to enable personal information removal under EU privacy regulation, available at https://policies.google.com/faq.

Appendix B: Digital Investigation for Financial Sector Executives

Introduction

This appendix documents the digital investigation described in 5.4 of Chapter Five 'Executive Risk'. Thirteen searches for high-ranking personnel from six eminent financial institutions are recorded chronologically to illustrate the challenges of digital research and the use of open-source techniques. All employees selected for investigation hold a senior post and typically have responsible for global services delivered by their organisation, although no official job titles are referenced, nor organisations identified. All personal data remains anonymous, and the individual may occasionally be referred to as 'the subject' to differentiate from other users who become an integral part of the search, for example, spouses or family members. Each search adheres to the parameters set out in 5.3.5 and the investigation follows a social engineering framework (Mouton, Leenan and Venter, 2016), using free and legitimate sources and tools to retreive material reffering to or posted by the individuals. Cyber-RAT evaluates user-generated images and text and any content published by acquaintances, the corporate employer or the online media to identify suitable target. Anonymised data suggesting potential risk of targeted social engineering attack was posted as a business report to each financial organisation (see 5.5). The report is available in Appendix C.

Search 1

The initial search for an individual at the highest level failed to achieve results (see 5.3.4), therefore an executive with a senior, but less high-profile position would be the next subject. An organisation was selected and entered as a

keyword in combination with “CEO”, “Director” or “Executive” in Google Advanced Search. This query returned biographies of senior executives published to the corporate website. Brief career histories and a photograph were available, using only first names and job title as the header, for example, ‘Simon, Director of Global Accounts’. A subject was chosen on strength of seniority, and the biography examined for usable information. The biography did not divulge the individual's surname, so the profile photograph was saved for a reverse image search (see 4.9.2) as other images on the internet might accompany written content and disclose the full name. As the image was being saved, it was observed that the upload to the corporate website had used the employees full name as the file title, instead of an anonymising jpeg number. Examination of all staff photographs ascertained that although the majority of images were anonymised, a few disclosed the full name of the individual.

The employees name was used as keywords in a people-specific search engine and results suggested a geographical area where the individual might reside. The geographical area and the full name entered into Google UK returned community newsletters containing the employees name published by a parish in England. The employees LinkedIn profile verified regular participation in their local (un-named) community as a recreational activity and the page biography listed the primary and secondary school attended by the user as a child. When the schools were used as search terms, both establishments were found to be in the parish publishing the community newsletters.

Public records identified other individuals with the same surname residing in the same locality. The names were entered into Google India so that any data restricted by EU data protection laws could be retrieved. This returned 'hits' from local news archives containing articles about the individual and relatives. Social media accounts for the subject and immediate family members were also retrieved. At the cessation of the search, the subject's spouse, sibling and immediate family members had been identified and the names and residential address of the subjects' parents was established. Community activities the couple were involved in, the location where they take place and the names of close acquaintances additionally involved in the activities were all known. Emails containing malicious attachments continue to be a "proven attack channel'' (Symantec, 2017, p.38) and an attacker might exploit the name and address of the subjects' parents in spear phishing correspondence. For example, an email purportedly from the local hospital or police station. Any reference to the spouse or other close family in association with an accident or another high impact event would likely evoke a reaction. The subject was particularly proactive in the local parish and reference to associates or community activities might convince the target of credibility and encourage access to any malicious attachments accompanying an email.

Other than the LinkedIn profile, little of the personal data retrieved during this search was published by the employee. The majority of information was found in content published by family, friends and online news resources, including community newsletters. The employees Facebook account used privacy controls on personal content but the list of Facebook 'friends' was accessible to all

viewers. Examining the profiles of ‘friends’ with unprotected social media accounts confirmed the family relationship with others in the same town. This highlights necessity for all members of a network to maintain privacy, otherwise social media use may position even an aware user in position of suitable target.

Search 2

Having ascertained that a corporation may have inadvertently breached an employee's privacy by disclosing their full name on an identifying image, it was deemed relevant to the concept of suitable target to explore how much information could be obtained about other users who may have assumed themselves to be privacy-protected. A second image disclosing a full name was selected from the corporate website and a keyword search using Google UK returned a link to Companies House (www.companieshouse.gov.uk) which established that the employee was a secretary for a limited company. The individual listed as the company director shared the same surname as the employee. In accordance with company law, public records listed the residence of both director and secretary and both parties shared the same address in an affluent area of London, suggesting that the couple are either related or married. A Facebook account in the employee's name was verified by a profile picture easily identifying the employee as the person on the corporate website. The timeline (the space on a profile where content is posted) contained little material and the ‘friends’ list was restricted by privacy controls, but the profile picture included a photograph of a new-born baby. Other users had posted comments about the baby image, and one included an active hyperlink leading to a publicly viewable profile with an accessible list of ‘friends’. A keyword search inside the ‘friends’ list returned the employee account and the profile belonging to the

individual sharing the surname who resides at the same address. This profile was unprotected by privacy controls and publicly accessible. From images and content, it was apparent that the account holder was also the parent of a new-born baby. It was therefore assumed that the two individuals with the same surname and same address were a married couple with a child.

Google India was used to explore the information obtained thus far. The two individuals had studied at the same university, both worked in finance, shared social groups and associates, and media evidence verified that the subject was related by marriage to a high-profile politician. Evidence could not be found to positively confirm that the politician was the parent of the subject's spouse, but the intelligence indicated that this was so. For an attacker, the information available about the spouse and baby, the London residence, the high profile relative or the name of the couples' business could provide credibility and convince the employee to respond to a targeted attack.

Searches 1 and 2 were significant for other than a professional LinkedIn profile, the subjects had little self-published content available on the internet and made effort to protect online privacy by protecting personal social media accounts. Data of value to an attacker was found amongst content published by friends and immediate family with Facebook profiles not protected by privacy controls. Other sources of data had been made available by the online media and public records and was out of the control of the individual.

Search 3

A third image disclosing an employee name was selected from the corporate website and keyword searches returned a recent interview given by the subject to the financial press and a Twitter account. Individuals often use the same username for multiple accounts, so Instagram was searched using the Twitter username as a keyword. An account was returned which used a modified version of the username but could be verified as belonging to the subject as the profile picture matched the image on the corporate website.

The Instagram account had no privacy protection and content was publicly accessible. Many images were of two young children and commentary posted by the employee revealed their names. The Instagram username was entered into Google India as a keyword and Pinterest and eBay accounts using the same username were returned as hits. The eBay account gave access to all the transactions made by the subject during membership of the auction site.

Thus far during the search, no information referring to a spouse or partner had been retrieved. The Facebook profile had privacy controls activated and the timeline contained little content other than a few comments made by ‘friends’. One comment referenced an unfamiliar name, so the profile of the user who had made the comment was examined. The friends list was accessible and contained the unfamiliar name. Open-source tools connected the subject’s profile ID number with the one maintained by the unfamiliar person and searched through Facebook for occasions where the two names appeared together. This method

retrieved images of family events where the couple were present and provided evidence to affirm (likely) status as a married couple.

The interview in the financial media had stated that the subject lived in a specific geographical area and social media accounts confirmed residency in a town in that county. The search for shared Facebook content using the linked profiles established that the employee and spouse had both 'liked' a community page maintained by a primary school in the same town. Public records divulged the subjects home address which was copied into Google maps. The school address was also entered into Google Maps and when the map was enlarged, it was evident that the primary school 'liked' on Facebook was one street away for the employee's home. As the content seen on Instagram suggested that the eldest child was of primary school age, and the school 'liked' by the parents in the vicinity of their home was (very likely) the school attended by the child.

This complete search took only thirty minutes and located the subject's immediate family, close friends, home address and most likely the child's school, all made possible using the corporate photograph as a starting point. This is significant for as the retrieved LinkedIn account had no profile photograph and without visual validation facilitated by the disclose of the full name, social media accounts could not have been verified as belonging to the employee. Despite some active privacy controls, social network profiles contained sufficient information for an interested party to execute a credible social engineering attack, possibly using the names of the children or the child's school. An additional concern is the use of the same username for all the online accounts – particularly the eBay account.

With access to data regarding items bought or sold, an attacker may deceive the subject by professing to be from a buyer or seller who the subject had dealings with on the auction site.

Search 4

This next search chose to use a millennial employee from the eighteen to thirty-four demographic with expectation of finding multiple social media accounts and an active internet presence. The subject was selected from biographies of senior level staff published on a corporate website. Surprisingly, the preliminary keyword search failed to retrieve a LinkedIn profile, and no social media accounts were returned as hits. The employees name was used as a search term on Instagram, returning many accounts with the same name. Despite the numerous accounts, the subject was easily identified from the image on the corporate website. The Instagram account had privacy controls activated, but an advanced search located images where the individual had been ‘tagged’ to other users' content. The ‘tags’ lead to another users unprotected Instagram account where images of the employee and friends from university were viewed. The friends were searched for on Facebook and a publicly accessible account provided access to the subjects Facebook profile which had been created using a nickname and subsequently not returned in the keyword searches. Comments and images on the timeline led to other users' accessible accounts containing content which identified the subjects partner, partners occupation and place of work.

As millennials are renowned for embracing internet trends (Gottfried and Dost, 2015) a substantial internet presence had been anticipated for the younger

financial employee, in addition to a possible disdain for privacy controls. The employee's millennial friends were ardent social media practitioners and behaved exactly as the millennial age group had been expected to, a profile on many different social networks, abundant personal content, ‘over-sharing’ and limited or absent privacy controls. In contrast, the employee had no LinkedIn profile a minimal amount of self-published content and social media account s which had to be sought rather than being returned as hits. Although sufficient data was retrieved to prove credibility (partners name, occupation and place of work) the content typically referenced lifestyle and friends instead of spouse and children. The differences observed in the internet presence of young professionals with similar lifestyles seen during the digital investigation conducted for Chapter Four ‘The Corporate World’ and that of the subject for Search 4 suggests that the financial executive may be complying to company policy regarding social media and internet activity. Such policies will be expected of all staff, but those in a senior role may be more inclined towards compliance.

Search 5

This search utilised the data made available in an employee biography on a corporate website as the starting point for the investigation. A high-ranking individual in a global postion whose biography stated that honours and masters’ degrees had been awarded from the same university was selected to be the subject. The employees name and the location and name of the university were used in a keyword string, returning a ‘hit’ mentioning the individual and spouse. The names were entered into a people-search database and a residential address and several links to articles published in the online media was returned. When used as a search term, the address retrieved data suggesting that the couple had

at least one child. Google India retrieved social media accounts in the child's name and unprotected profile pages contained photographs confirming a definite family relationship.

The media articles followed a pattern of publication each time the employee took a new and higher position in a different organisation, so the employment history was used as search terms. Archived biographies published to the previous employers corporate website were retrieved. Information from the earliest biography revealed that the individual had four children and a search inside Facebook located two young people with the subjects surname who lived in same town as the residential address. The Facebook account ID numbers were connected using open-source tools and a search for other family members retrieved a third name confirmed to be the employee's mother. The mothers name as a search term returned an obituary for a family member where all four children, siblings and other relatives were named. The fourth child could not be found on social media, but keyword searches using data from the children's profiles identified the school attended by two of them. The fourth child's name appeared in sports teams based in the same location as the school, suggesting that this child was also a pupil. A further keyword search using the combined information about the family revealed that the subject's sibling was a global name with a high-ranking position in a well-known establishment.

This search, facilitated by innocuous information available on a company website, provided ample data specific to the employee which might be exploited by an

offender. Names of parents or siblings in conjunction with the name of the village where the family live or the children's names and their school might evoke the opening of an unsolicited email. This particular subject had a long and prestigious career in the financial industry and the heritage biographies retrieved from corporate websites provided data that an attacker might abuse. A claim to a mutual friendship from previous employment might entail the attacker being accepted as a social media friend. Attackers abuse trust (Hadnagy, 2010) and the data available in the corporate biographies could enable an attacker to create a convincing charade.

Search 6

The next search attempted to locate employees using documents published online, for example an annual report and accounts. Google UK was used to search for PDF files for a selected financial organisation and retrieved the most recent annual report, press releases and other internal papers. Searches were conducted inside the content of the PDF files and 'hits' for members of the Corporate Governance Team were returned. Team members names were entered as keywords, but no personal data was retrieved, only commentary from the online media. The annual report referred to a 'Senior Management Team', so this phrase was entered into Google Advanced Search engine. Staff biographies from the corporate website were returned but provided no suitable data to progress the investigation. Using the team members as keyword searches returned nothing more than professional references in online media, for example, an interview commenting on a financial issue or mention of a new appointment. Although all members of the senior management team had LinkedIn profiles, they did not list their employment history, only the current employer and no other

personal data to use as keywords. As employees from this organisation were proving difficult to locate, a search was conducted on all names of senior-level employees published on the corporate website. Eventually a LinkedIn account was returned showing a professional resume which might be used as keywords, but the account had no profile photograph. Without an identifiable image, social media accounts or other internet resources could not be confirmed as belonging to the individual.

The investigation had reached an impasse and it became necessary to take advantage of the 'recommendations' feature provided by LinkedIn. Whenever a profile is accessed, the LinkedIn algorithm recommends other users connected by industry, organisation, or hierarchy. The user-account without a profile picture was for an executive member of staff and consequently LinkedIn provided links to other senior personnel from the corporation, some of whom had published photographs to accompany their biography. An executive was selected randomly, and the data published to the biography used for keyword searches. Several Facebook accounts were returned maintained by users sharing the same name and each one was examined individually. The subject's profile was confirmed by self-published selfies matching the user in the photograph on LinkedIn. Privacy controls protected the list of 'friends', but the timeline was accessible and family members were identified from content. Family profiles had no privacy controls and comments made by the subject and others divulged significant personal details including a recent family death, a birth and an engagement. Open-source tools were used to connect the profile of the employee with other family members and the subject's partner was identified. The partner had a very active online

presence and maintained three publicly accessible Facebook profiles. The accounts and revealed the address of their workplace alongside a personal association with several well-known television personalities.

It has been observed throughout the searches thus far that the members of a subject's social network will typically provide access to data confirming family relationships. For social engineering to succeed, an attacker must convince a victim of credibility and regular contact between family members may invoke another method of attack. A social media friendship initiated with a family member using personal details harvested from accessible social media accounts may facilitate sharing and spread of malware to a valuable target located in an organisation.

Search 7

The list of profiles recommended by LinkedIn during the previous search was perused again to find a senior employee with a profile photograph. The first keyword search returned nothing except articles in media archives celebrating new appointments made within the corporation and heritage interviews from earlier in the subject's career. No personal data was included in the content. No social media accounts were retrieved, a reverse image search found no similar images and the LinkedIn profile contained only a brief resumé of the career path. The employees name was entered into an advanced search engine which retrieved another media article which made a brief reference to a sporting activity. The sport and the subjects name as keywords returned several ‘hits’ of results

from races published on a sports website. The subjects name was listed accompanied by a second individual sharing the same surname.

The second name was used as a search term and retrieved several Facebook accounts maintained by users with the same first and last name. Accessible content on the profiles was briefly inspected for any comments or images referencing the sporting activity. One profile timeline contained a photograph of the account holder participating in a similar sporting activity, so this account was examined further. The ‘friends’ list was unprotected by privacy controls but no others in the users network shared the surname. Open-source tools connected the profile to other users in the ‘friends’ list but no evidence of a family relationship was found. The timeline contained photographs of the user performing in a group of amateur dancers and a group of performers depicted on another page had been ‘liked’ by the user. The name of the troupe was researched using Google and the employees name, the name of the Facebook profile holder and the dance group were used as search terms on Google Advanced Search. This returned an online review posted to an events website where two people had left comments after participating in an event. The review included a clear photograph of the two people, and the identity of the employee was verified using the LinkedIn profile pictures. The identity of the second person was confirmed from photographs on the Facebook profile and the online review confirmed a family relationship.

Using the employees name and the hometown of the dance troupe as keywords retrieved a human-interest interview where the subjects’ spouse and the

geographical area where the couple had previously resided was mentioned. The spouses name as a keyword returned several recent ‘hits’ where the name appeared in articles about community groups based in the same geographical area. Combining all three names as a search string retrieved a blog entry where the blogger referred to the complete family by name, including a second child. No social media accounts could be found for the second child although the name was found on a blog maintained by a school in the same area.

Public records provided a partial address where the two adults might reside. The children were not listed as residents, suggesting they are too young to be included on the electoral register. This may be why the second child could not be found on social media as they were too young to hold an account. A search string using the employees name combined with the partial address revealed a dissolved directorship of a limited company. In compliance with company law, a full address was recorded for correspondence purposes and retained as archived data in a government database. Google Maps revealed that the residential address, school, community groups attended by the spouse, and the performing arts troupe frequented by the eldest child were situated in a small locality. Public land records showed that the property at the listed address had remained under the same ownership for two decades, implying that the employee lives at the address and the family are actively engaged in the local community.

This subject was a high-profile executive with a critical role in a global organisation and the lack of personal internet activity suggested an intention to

retain privacy. Family members disclosed no direct link to the subject and social media profiles attempted to control privacy, nonetheless, This search illustrates how tenacious online research can obtain data of value to an assailant, despite a subject having no obvious internet presence. An attacker might exploit information pertaining to the spouse or children, community or sports groups, the child's school, or even local area incidents affecting residents as internet resources had verified where the subject lived.

Search 8

The next subject was an executive at the most senior level of the chosen organisation and as expected, the preliminary search returned no information of value. Despite this, a fragment of heritage information transformed a failing enquiry into an investigation which reached a satisfactory conclusion.

The Boolean string "chief" OR "senior" OR "director" OR "president" OR "executive" AND "name of organisation", site:linkedin.com returned photographs of the leadership team posted to the corporate website. A subject was selected and keyword searches using the employee and the name of the organisation returned articles in the online media. These were industry-based reports and provided no personal data. Google UK did not retrieve any social media accounts nor did searching using the employees name inside Facebook and Instagram. The media articles were re-examined and observed a brief reference to a foreign posting prior to moving to the current position. The country where the employee had been posted combined with their name as search terms, retrieved a general interest article published by local press resources from a city in a specific area of

the UK. The article made it clear that the city was the subject's hometown and provided the name of the employee's spouse. The employee and the hometown were entered into Google India, returning a list of Facebook accounts held by people sharing the same name who also lived in the city. These were accessed individually, and the employee profile was identified from images matching the picture on the corporate website. Keyword searches for the spouse retrieved no data.

The Facebook profile had no privacy protection and the accessible ‘friends’ list identified one of the subject's parents. The parent's account was private, but the profile picture was a family gathering and all attendees were ‘tagged’ with their full names. The spouse did not share a surname with the subject, which was why no results were retrieved when searching for the name. Open-source tools connected the employees account with others from the ‘friends’ list, and content was found to confirm the spouse's identity and names of two of children. Keyword searches revealed that the couple were director and secretary of a limited company and public records provided a correspondence address. This was examined on a housing website and confirmed to be a domestic property rather than an office address so was assumed to be the family residence.

The employees Facebook ‘friends’ were examined for users sharing the spouse's surname and this identified the parents. Accessible content available on the parent's timeline referred to a street location in a nearby town, where the employee and family allegedly spent a lot of time. Google India retrieved a recent

planning application for permission to redevelop a property in the same location. The application had been submitted by the subject and spouse, and the form gave the full address of the property.

This search was facilitated by one fragment of heritage data referring to a foreign posting and unprotected content on other users' profile pages identified the subjects' extended family, two children, a spouse who had attempted to remain anonymous, the addresses of two properties and a business. The users revealing the critical data identifying the spouse, the children and the location of the second home were older members of the subject's family. The grandparents had posted photographs of the employee's children and other people had added comments revealing the children's identities. This is an example of how awareness should be raised whenever someone unfamiliar with the threats of the internet is encouraged to use social media. Older family members undoubtedly benefit from sharing in family news and events, but social media users should be informed about privacy controls and the necessity to remain vigilant at ensuring they are active. Social media platforms regularly update their systems and privacy controls are often affected.

An attacker creative with words may persuade a recipient that a semantic phishing email is genuine, but access to a target may also be achieved by misusing credible images. Using results from this search as an example, an attacker might copy a photograph of the children with their grandparent from Facebook. It could then be sent as an email attachment to the subject, using their names as the

subject heading. A personal family photograph sent to a corporate email account would raise alarm or pique curiosity. A parent will instinctively react to an image of their children and the email would most likely be opened. Other creative phishing might include the address of the second home as the title and a faux email from a ‘neighbour’ claiming a break-in, storm damage or flood, or include names of the subject's spouse or spouse's parent. The spouse did not share the employee’s surname and it might be assumed that only close associates would be familiar with the marital relationship. An attacker using the spouses full name in an ‘urgent’ email might persuade the target of credibility.

Search 9

This search is significant as very little data could be found about the subject's professional career and private life. If outdated information had not been retrieved from heritage sources, this investigation would have been abandoned. The search string “chief” OR “senior” OR “executive” AND "name of organisation" in site:linkedin.com retrieved profiles for senior-level positions. The chosen subject and corporation name entered into Google UK returned links to media archives reporting on the subject taking new positions within the industry. The search was repeated with Google India and again, only references in the financial press were returned. The media reports indicated an appointment as non-executive director of an associated company, but public records showed a resignation from the position and the correspondence address was the company office rather than a residential property.

The LinkedIn profile showed only the current employment, but the biography history showed past association with charitable organisations and provided the dates the collaboration had occurred. Names of the employee, the charity and an operator to return PDF files entered into Google India returned archived documents relating to charitable activities. Files corresponding to the dates seen on the LinkedIn profile were downloaded and keyword searches conducted within the documents. A report dated from 2008 included brief biographies of charity associates and the one relating to the subject disclosed the names of the spouse, stepchildren and the city of residence twelve years previously. The names of the subject and spouse as keywords retrieved an archived media article regarding the subjects wedding and disclosed the spouse's maiden name.

A search was conducted inside Facebook using the name of the subject, spouse, stepchildren, corporation and the maiden name. Several profiles were returned and were examined individually to eliminate any which could not match the subject because of ethnicity or age. The LinkedIn profile picture was the only image available for identification purposes and was not a professional photograph but a casual amateur image. Facebook profiles were perused until data matching the search terms was identified and an unprotected profile eventually confirmed as belonging to the employee. The content included comments from users with names matching the spouse, stepchildren and other family members sharing the maiden name. The profile page assumed to belong to the spouse was private and contained no content. Open-source tools connected the account to that of the employees and retrieved content which the two parties had both ‘liked’, mainly images of the stepchildren. A brief search in Instagram for the subject located an

unprotected account which contained no content. The account followed other users and appeared to have active followers. Perusal of the list of users connected to the account revealed Instagram profiles held by the stepchildren and the subject's siblings, none of which were protected by privacy controls. The stepchildren's Facebook accounts were also unprotected and accessible.

This search demonstrates how passive footprints may subvert any intention by a user to maintain privacy on the internet. The employee had (apparently) made effort to keep self-published content to the minimum and may have been confident of avoiding inappropriate monitoring. In this instance, old documents provided data to uncover the employee's family, despite the information in the documents being out of date and published more than a decade previously. Normative searches retrieved no personal data about this employee who may have considered their internet presence to be adequately protected. Subsequently, an attacker using the names of the spouse, children and family in targeted spear phishing might convince of credibility. The names were not public knowledge and could not be retrieved with simple search methods. The unprotected social media accounts maintained by the subject's family might be an additional avenue of an avenue of attack. The accounts provided adequate data to claim a mutual or actual acquaintance and might provide eventual access to the high-ranking employee.

Search 10

It was observed throughout the digital research in both Chapters Four and Five that users with pleasing facial features tended to be ardent social networkers with

profiles on multiple platforms and often a lack of activated privacy. This suggested that attractive users are engaging in the social media narcissism described in the literature (Bergman et al, 2011; Carpenter, 2012, Wang, 2017). It was therefore decided to attempt a search without an assumption of available data made possible by user typology, and the subject for Search 10 was selected on merit of their surname rather than visual features seen on a profile picture. To enforce this, LinkedIn was not accessed during the search. The Boolean string “chief” OR “senior” OR “executive” AND “name of organisation” was used to find an employee with an uncommon name. Keyword searches returned links to the online media, but articles were not about the subject per se, and instead referred to their specific occupation. No personal data was made available, but images accompanying articles enabled visual confirmation of identity.

The employee name as a search term in a people search engine retrieved data about the university attended by the subject and the university name, the subjects name, occupation and organisation were used as a string to search inside Facebook.com. A corporate profile was returned which had been ‘liked’ by the subject, thus confirming the existence of a Facebook profile. Open-source tools were employed to retrieve any images posted by users sharing the employee's surname. The images were examined individually, and the subject was recognised from the images used in the media articles. Without the information made available by the media, the Facebook profile account would not have been found, as the profile pictures used on the subjects’ page were of family members and holiday landscapes.

The profile page had no privacy controls activated, and the friend's list and all timeline content was accessible. Comments posted by the subject and 'friends' disclosed personal information including the parents and their location, siblings, and voluntary activities undertaken in the employees spare time. Data from the Facebook profile used as search terms retrieved a Twitter account and although the content was not accessible, the employee had 'followed' a small group of Twitter users. When these accounts were examined, they were also volunteers associated with the voluntary activity. Using the Twitter username as a search term retrieved an account on Instagram with no privacy protection and no content but with a list of accounts followed by the employee. These were family members and more volunteers involved in the voluntary activity. The Twitter and Instagram username was entered into Google India and results indicated a directorship of an independent company. Public records confirmed the directorship, and the correspondence address was cross-referenced using public databases. An individual of the same age and name was recorded as resident in that property.

Although access to profile images may greatly expedite the identification process, this search demonstrated that LinkedIn need not be a quintessential requirement of a people search. If an individual does not self-publish content, other resources can provide sufficient visual content for identification and verification purposes. From the perspective of the social engineering attacker, this search obtained ample data relating to the subjects' personal relationships. Both parents were named, alongside photographs of their home and information about the area where they reside. Close relationships with siblings and the group of volunteers were identified. A targeted attack referencing the parents or containing a family

photograph copied from Facebook would cause alarm and invoke reaction to the email. Details regarding the voluntary group would attract the employee's interest or an attacker might reference the employee's independent company to convince of credibility.

Search 11

Search 10 described above had consciously avoided choosing a subject on the merit of their appearance and instead focused on any data available online about the subject. This next search would take the opposite approach and deliberately seek a subject suggesting social media narcissism (Bergman et al, 2011; Carpenter, 2012, Wang, 2017). The intention was to determine whether an attacker might capitalise on the knowledge that attractive users produce abundant user-generated content and include a pleasing appearance as criteria for suitable target.

The string "chief" OR "senior" OR "executive" OR "director" AND "name of organisation", site:linkedin.com was entered into Google Images. This returned LinkedIn profile photographs which were examined for the attributes observed in searches where personal data was successfully retrieved. The name of the chosen employee was entered into Google Images and retrieved other photographs available on the internet. The pages associated with the images divulged the area where the subject resided. Facebook was explored using the names of the individual, organisation, and location of residence and the employee's profile was easily recognised from photographs found by Google images. Unprotected content revealed the name and age of the subjects' young

child and identified a sibling who also maintained an unprotected profile where the names and locality of other immediate family were available. Entering the names of the sibling and the subject into Google India located the obituary for a recently deceased grandparent and identified all the remaining family members.

This search is significant as the senior executive subject was from the millennial demographic and selected for an image displaying attributes typical to social network users who ‘over share’ (see glossary) on multiple social media sites. The investigation took very little time to reach an effective resolution as all social media accounts were publicly accessible with abundant content provided by the user and augmented by comments posted in response to the content. In common with the previous searches, the personal data located is adequate for an attacker to create credible emails by referencing the subject’s child or family members.

Search 12

To continue with the use of images as the preliminary search tool, it was decided to revisit corporate websites and ascertain whether other organisations had breached privacy by publishing images inadvertently disclosing an employee's full name (see Searches 1, 2, and 3). All websites maintained by the chosen financial organisations were examined and a second company was found to be publishing image files containing surnames, despite all reference on the website being limited to a first name only.

A reverse image search using the photograph of the selected executive found no further images, indicating that without the full name published by the corporation, identifying the person in the photograph would not have been possible. An advanced keyword search inside Facebook retrieved the profile with no active privacy controls in place and accessible images with comments left by 'friends'. Examination of the images verified photographs of the subjects' siblings and parents.

Many images of university friends were posted to the profile and comments posted by the subject clearly indicated close relationships with other users. One comment included a social media username prefixed by a hashtag. The name was used as a keyword and because the employee was 'tagged' to content on another users' page, their Instagram account was retrieved as a 'hit'. The accessible account displayed photographs observed as characteristic for users of both genders aged between twenty-five and forty years old employed in high-ranking positions with no marital responsibilities or children. The images were of exotic travel destinations, nightclubs, music festivals and other lifestyle experiences with family and close friends all of whom were identified by name and tags to active Instagram accounts.

Visual data available on social networking sites can provide multiple streams of potentially credible data. For example, an attacker could imitate a friend followed on social media or from university, and comment upon events portrayed in the images, thus gaining trust. The assailant could pertain to be a friend or acquaintance of the parents and use visual information as content for an email.

Referencing events, images or experiences from Facebook and Instagram or copying images from the sites and including them as attachments will most likely convince a victim to open an email.

Search 13

As the exploratory search documented in 5.3.4 had failed to find data about the highest-ranking executive in a corporation, the final challenge to conclude the practical research would use media archives as the primary resource and aim to establish the most senior executive in the selected company as suitable target. To locate personal data it would be necessary to examine the employees early career and find human-interest data used by a journalist to illustrate their personality. Google Australia settings were modified so that the preliminary search would be conducted in news archives, and a custom timescale was set to focus upon the previous ten years. Keyword searches using the names of the employee and organisation returned multiple ‘hits’ from variable sources including local journals and financial press. Each item was examined to identify elements of general interest intended to illuminate the subject. Data was found referring to a location of former residence, a personal interest and a hobby. These became key words in a Boolean string and a heritage article from the Financial Times was retrieved where the first name of one the subjects’ children was included in the text.

Adding the child's name to the keyword searches retrieved the geographical area where the employee resides. An image search for the local area returned pictures of community events and a photograph included the subject and identified the

spouse. An advanced search was conducted inside Facebook using all found names as enquiry terms and retrieved the account belonging to the spouse. The 'friends' list was privacy protected but the timeline content was accessible, and immediate family members were identified from comments and images. The profile maintained by family and close acquaintances were similarly accessible and provided sufficient information to locate the Facebook and Instagram profiles of the employee, despite the accounts being disguised by a pseudonym. At the conclusion to the final investigation the spouse, both children, parents, grandparents, siblings and extended family had been identified. The employees residential address and the address and location of both schools attended by the children were known, alongside names and addresses of close acquaintances involved in community interests.

From the information available on social media a credible attack could be launched against an individual with access to significant corporate resources. Family-specific data harvested from the unprotected social network accounts combined with names of the employee's parents or siblings might incite the opening of an unsolicited spear phishing email. Misuse of the children's names and their schools may also provoke a response. The spouse and children were very active on social media and regularly posted information about current activities and the locations where they were shopping, eating, or visiting. This type of content might be used to convince the spouse of mutual acquaintances or interests and an attacker could be accepted into a social media friendship group. By socially engineering the spouse, an attacker might gain access to the employee.

Despite using pseudonymous social media profiles in effort to protect their online presence, the highest-ranking executive in a global financial corporation had no control over content produced by others. Family members and other close acquaintances divulged personal data of value to an attacker. Although heritage data enabled the family profiles to be found, privacy protection would have prevented personal information from unsolicited public access. It has been observed throughout the practical research that parents and grandparents use Facebook to remain in contact with family located all over the world. Grandparents are often social media 'friends' with grandchildren while parents are not granted that privilege. This again highlights the importance of ensuring that all associates in a network of friends or followers are conscientious with privacy as a single accessible account may compromise a carefully maintained web presence.

The searches documented in this Appendix have been synthesised in section 5.4 of Chapter Five, 'Executive Risk' and visually illustrated in Table 3 (5.4.4).

Appendix C: Report Sent to Financial Organisations

January 2018

Internet Presence, User Generated Content, and Spear Phishing Attacks.

A Risk to Employees and Organisations.

Raichel Collis
UNIVERSITY OF DERBY

Table of Contents

Executive Summary.... 5288

Introduction 529

Overview 5299

Methods..... 53030

Findings 53131

Observations 53232

Conclusion..... 53232

Recommendations ... 53333

Additional comments53333

References 53434

Contact Details.....534

Executive Summary

Spear phishing emails are aimed at individuals or selected key targets within an organisation, and an attack will succeed if the email contains credible content which convinces the recipient of legitimacy. This report documents an exploratory internet investigation, which was conducted in October/November 2017, and intended to identify whether executive-level financial employees are at risk of targeted social engineering attacks.

The public internet presence of thirty-five senior executives from six eminent financial organisations was examined. Free and publicly accessible internet resources, including search engines, news archives, social media and user-generated content were used to seek key personal details suitable for exploitation during a targeted attack.

The report finds that over 50% of the employees revealed personal information amongst content available on social media sites and other public websites. Names, significant details, and visual images pertaining to spouses, children, parents, siblings, and other crucial facts, were accessed from open sources. Use of such data by an attacker could potentially provide the credible content which would entice a victim to open a phishing email and any attachments containing malware. A successful attack could compromise the corporate IT network, alongside corporate and customer data. Each of the selected organisations employ executive level staff who may be considered a risk.

Recommendations include:

- **Review of employee social media policies with emphasis on amending privacy controls.**

- **Awareness raising amongst staff to highlight the importance of retaining control of personal content.**

- **A reassessment of insider risk caused by employee use of technologies.**

Introduction

The financial sector is alert to the threat of cybercrime, and as such, corporations expect that employees practice good cyber hygiene when using the internet. Organisations using digital systems have policies and procedures in place governing mobile device use, social media, and online activity. However, despite safeguarding efforts, emails containing malicious attachments continue to be a "proven attack channel'' (Symantec, 2017 p.8). Threats aimed at either an individual or a few selected targets within an organisation are expected to rise (Symantec, 2017 p.38). Such targeted attacks are known as 'Spear Phishing'

A phishing email is constructed to instil a sense of urgency, compelling the recipient to react, without assessing if the email is legitimate. Professionals may have received awareness training regarding spam and phishing emails and will be suspicious about unsolicited messages. Therefore, an attack can only succeed if an email contains plausible content which convinces a cautious recipient of credibility. In the contemporary networked society, users make vast amounts of personal information easily accessible to any interested party. For this exploratory exercise, conventional internet search methods were used, alongside publicly accessible open sources. Searches obtained critical personal information about key personnel within the financial sector, indicating that those individuals may be an inadvertent risk to their corporate IT network.

Overview

The aim of the exercise was to establish whether personal data could be identified amongst content published on the internet. The typical internet user may not comprehend the amount of information about them which can be found online (Hadnagy, 2010), nor the type of data an attacker would exploit when preparing for an attack (Junger, Montoya and Overink, 2016). As such, avid users of social media place vast amounts of personal information onto public platforms. Even those who exercise caution in their online activity may be surprised by the quantity of information made available from other internet users or from public records. It was intended to ascertain whether an attacker could use the available data to create a credible spear phishing attack against an executive level employee from the financial sector.

Methods

Six eminent financial organisations with a strong UK presence were chosen, and thirty-five executive level personnel identified by using typical internet search methods. Individuals were selected on merit of senior positions in their organisation. They were of varying ages, cultures, gender, and all were based in the UK.

Open source internet resources were then used to search for personal information which might persuade a target that an attacker was personally acquainted with themselves or their family. The information sought included:

- Names of spouses and partners.
- Residential addresses.
- Names, ages, and schools attended by any children.
- Close relationships including parents, siblings, close friends, and associates.
- Hobbies, community and social activities, clubs, societies, or groups attended by the individual, spouse, children, or other family members.
- Visual images.
- Key facts and dates e.g. birthdays, weddings, deaths etc.

Only legitimate, ethical, and publicly accessible internet resources were used during this research experiment. These included Google, media archives, Facebook, Twitter, Instagram, and other free sources obtainable online. The researcher is familiar with methods used by open source investigators; however, these techniques do not involve the use of additional or third-party software. All open source tools and facilities used for accessing and sorting data were freely available on the internet. The digital content included images and text published by the individual, acquaintances, corporations, and public bodies and was available on social media, websites encouraging user interaction and public databases.

The initial search for data took place for thirty minutes, if no data was obtained in that time, the individual was withdrawn from the investigation. If personal information was found, the investigation continued until sufficient data to create a credible email was collected. No search continued for more than 2 hours.

Findings

Thirty-five senior employees were researched, and nineteen individuals were considered to have sufficient information available about them to be at risk of a social engineering attack. All the selected organisations employed at least one or more individuals who made critical personal information available online. Personal information was most frequently published on social networking pages without active privacy controls. Other information was available on media archives or public records.

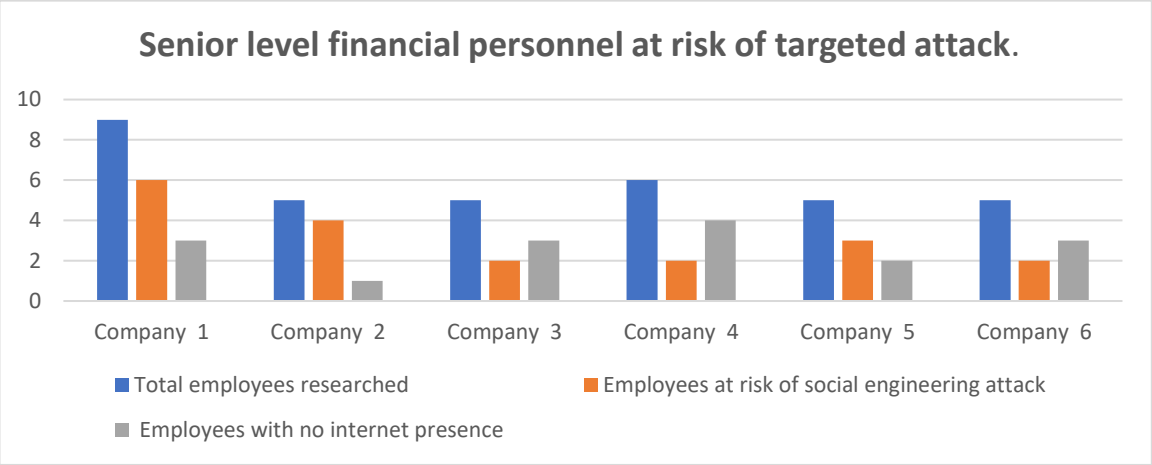

Figure 1 Executive level employees from financial organisations

The personal information obtained during the investigation included images, comments and key facts about spouses and partners, immediate family and children, close relationships, community groups, and social activities.

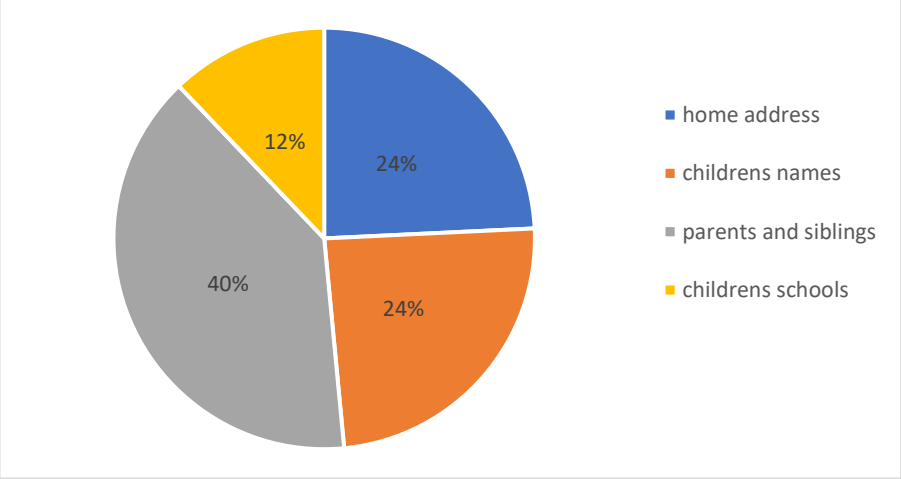

Figure 1 Personal information obtained about 19 executive-level employees

Observations

1. Much of the key data was retrieved from comments or content posted by individuals, friends or other third parties, and intended for public viewing on social media sites. The majority of profiles viewed during the research were unprotected by privacy controls.
2. On occasions when an individual did protect their own social media profiles, comments posted on a profile page by others would often lead to pages maintained by close family members or acquaintances. These pages were generally unprotected by privacy controls and often contained personal details linked to the individual.
3. Older family members are more likely to reveal personal details about relatives and make all content available for public viewing, including lists of friends and followers.

Conclusion

The overall intention of the research was to establish whether an attacker could create a credible targeted attack from critical personal data published amongst online content. As an example, an email using information about a child, allegedly sent from the child's school, may provoke an immediate response entailing the opening of a phishing message and any malicious attachments. An email using names of a spouse, children, parents, or the home address and including family images downloaded from a social networking site may also cause an instinctive reaction.

It should be noted that the information observed during this research was found using normative search techniques. A tenacious internet criminal may also use illicit methods or third-party software to obtain the information needed for a phishing attack.

Recommendations

1. The findings of the report recommend that employees are advised to re-address their privacy controls on all social media profiles and to advise any friends, family and associates who may post on their pages to do the same.
2. Individuals should be cautioned against posting content referring to their children on profiles not protected by privacy controls.
3. Older family members who have been introduced to social media as a method of social and family inclusion, should be guided towards available privacy controls and cautioned against divulging personal content on the internet.
4. Organisations should consider a reassessment of insider risk caused by employee use of technology. This should include the use of personal mobile technologies in and out of the workplace and devices associated with the Internet of Things.

Additional comments

This exploratory research has been conducted for the sole purpose of indicating to financial organisations that there may be unexpected risks created by employees and technologies. It is hoped that the findings of this report will persuade those responsible for information security of the value in recommending that personnel from this organisation become anonymous volunteers for a doctoral research study. The doctoral research is investigating how employees in the financial sector use personal technologies and Internet of Things devices and whether this has the potential for unexpected impact on the IT network. Any participating organisation will receive a copy of the aggregated findings to use for amending policies and undertaking risk assessments.

The data contained in this report will be used as part of the doctoral thesis and has no other purpose. All individuals associated with this research are anonymous and no record has been retained of their names, job titles, nor the organisations they are employed by.

References

Hadnagy, C. (2010) *Social engineering: The art of human hacking*. Indianapolis, IN: Wiley.

Junger, M., Montoya, L. and Overink, F. (2017) 'Priming and warnings are not effective to prevent social engineering attacks', *Computers in Human Behavior*, 66, pp. 75–87. doi: 10.1016/j.chb.2016.09.012.

Symantec (2017) *2017 Internet Security Threat Report*. Volume 22 Available at: https://resource.elq.symantec.com/e/f2 (Accessed 11 January 2018).

Contact Details

Raichel Collis. PhD Candidate. r.collis@derby.ac.uk

Dr David Hicks. Director of Studies d.hicks@derby.ac.uk

Appendix D: The Impact of the Change in UK Data Protection Legislation

Introduction

Chapter Six ‘A New Direction’ recorded the methods that were necessary to continue the digital investigation and seek a sample purposely selected for suitability to answer the research questions. These new methods (see 6.2) were distinctly different to the original research proposal and clarification was sought from the project supervisory team to ensure that the research ethics approved in 2017 would similarly apply to the new proposal. This was pertinent because the General Data Protection Principal (GDPR) had passed into law on 25 May 2018, replacing Data Protection Directive 95/46/EC with a single set of data protection rules (GDPR, 2018) subsequently superseding the Data Protection Act (1998) with the Data Protection Act 2018.

Pre-GDPR Dates

To understand the impact of the new data protection legislation on the project, it must be explained that the preliminary preparation for Post Graduate research commenced in December 2015 .The application for ethical approval was submitted to the College Research Ethics Committee in November 2016 and approved in April 2017 in accordance with the current UK legislation, the Data Protection Act (1998) (DPA (1998. The open-source research documented in ‘The Corporate World’ and ‘Executive Risk’ was completed in 2017 and followed the data protection principles of the DPA (1998). The business report (see Appendix C) compiled from the results of the investigations in ‘Executive Risk’ (see 5.4 and Appendix B) was sent to the selected organisations in January 2018.

The original electronic survey was built in February 2018 using DPA (1998) compliant software purposely selected for the privacy and security offered by the survey provider. The financial organisations who initiated contact with the researcher all requested and received the link to the live survey prior to May 2018.

Repercussions

The introduction of the GDPR had unanticipated repercussions when the pursuit for primary data pushed the methodology in the new direction documented in Chapter Six. The impact was exacerbated by a change in the project supervisory package and a new team member viewed the research instrument and associated documentation for the first time. The fresh perspective triggered a review of the electronic survey and documents, for although fully DPA (1998) compliant, the additional criteria required by the GDPR was absent. To ensure that any ongoing practical research would be fully compliant with the new legislation, a second application for ethical approval was submitted to the University Research Ethic committee. The research instrument, letter of invitation, participant information and debrief documents were all revised to ensure compliance.

Requirements for GDPR: Survey and Documentation

The GDPR is not a complicated piece of legislation, but the introduction of new procedures caused apparent confusion when applying the guidelines to academic research. To achieve compliance, the respondent information sheet required amendment to include essential information regarding industry standard encryption, data protection, survey provider compliance and other relevant details to inform how collected data would be used. The detailed information was a necessary provision to inform participants of rights under data protection law. The

consequence of the additions to the documentation was that a lengthy explanation now appeared on the first page of the electronic survey. Any respondent using a smartphone to access the questionnaire was required to scroll through several screens of text before reaching the option to provide informed consent. Much of the GDPR criteria was later repeated in the debrief document at the survey end, where contact details were provided for the Data Protection officer at University of Derby, the researcher, and Director of Studies.

Right to Withdraw

An integral requirement of the research design was that respondents would be assured of complete anonymity. The survey software had been selected for confirmed data protection compliance and could be configured to ensure that no personal data, IP addresses nor email addresses would be captured. Since no identifying data would be collected, the original application for ethical approval had been granted without offering respondents the right to withdraw. To offer withdrawal would require a method to identify specific data and subsequently specific respondents, thus voiding the assurance of anonymity. The original survey was built with emphasis on informed consent and respondents were advised from the outset that there was no right to withdraw. Consent was given on this understanding.

An assurance of anonymity was key and needed to be maintained, but requirements demanded by the GDPR stipulated that all respondents must be offered the right to withdraw as default. As a solution to ensure compliance participants were advised to create and enter a unique code. The six-digit

identifier would then be recorded by the respondent to be quoted in any email requesting withdrawal. The right to withdraw would be available for fourteen days after survey submission. Data would then be amalgamated, rendering it impossible to withdraw individual responses beyond that time.

Amending the Electronic Survey

The e-survey was already live and could not be modified, a result of the original testing process when pilot testers had submitted their responses during fault-finding exercises. Although their data had been removed before the survey link was shared with Banks A and B, the software package prevented any alterations to the construct. To enable modification, a copy was created, and the amendments inserted into the new version. In addition to the GDPR revisions, the overall content was improved. Scaling methods were introduced, and skip logic and pipes were enhanced. To reflect evolution in consumer technologies, the questions were updated and revised. As an example, in 5.2 it was explained that voice activated virtual assistants (Alexa or Siri) had been added as a revision since demand for the technology had made them popular items. In the short time that the survey had been live, virtual assistants had evolved further to become voice activated operating systems for home IoT devices. Rapid changes in technology had to be accommodated so that theorising of contemporary risk was possible from the results.

The Ethics Application

The recommendation to make a new application for ethical approval was unexpected and the decision to apply was made shortly before the College Research Ethics Committee was to convene for the first sitting since the

introduction of the GDPR. To satisfy a committee nervous about penalties for failing to implement changes to data protection subsequently necessitated strict adhesion to all available guidelines. In addition to soft copies of the amended research instrument and documentation, an application form documenting (in detail) the proposed research methods was required. The late decision to apply for approval demanded that all amendments to the survey and documents must be implemented in only seven days. To assist with completion in the limited time available, the application for ethical approval approved in 2017 was revisited since the proposed research methods were succinctly described. GDPR compliance amendments were inserted into the original text and highlighted for ease of reading. The proposed new methods for data collection were included for assessment and approval. The e-survey was downloaded into a Word document and all documentation was attached as appendices. The completed application was approved and signed by the Director of Studies who returned it to the researcher on the morning of the deadline for submissions.

The preparation for new ethical approval coincided with the introduction of new postgraduate software expected to improve the student research experience at the University of Derby. All ethics applications were to be submitted electronically, rather than hard copy and the intention was to upload the amended 2017 application to the researcher's student account. Whilst attempting the upload it transpired that no pre-existing documents could be entered to the software. Instead, the new system required an online template to be completed as a new document for submission. The researcher informed the University Research Office that the application was already complete and could be emailed direct to

the College Research Committee. The Research Office refused to receive the application and insisted that only the online template would be accepted, leaving no option but to create a new application to reach the committee before five p.m. that day.

The electronic template was formatted differently to the original 2017 form and attempts to copy and paste appropriate content resulted in an unintelligible application with no coherence. The only solution was to create a completely new document as dictated by the Research Office. The 2017 file was then reconfigured so that documentation and research instrument could be formatted for insertion into the digital version. Under the new system, all ethics applications using the new software would automatically be directed to the students Director of Studies (DoS) who would approve, sign, and take responsibility for advancing to the Research Office. With the DoS pre-warned and prepared to receive the document, the application reached the Research Ethics Committee twenty minutes before the evening deadline for submissions. The research was granted ethical approval four days later, enabling data collection using the new methods to proceed.

Appendix E: Letter of Invitation

Dear ……

The Ask: Please participate in a PhD research project on employees and the use of personal technologies.

Why? Smartphones, tablets, iPads and other internet-connected devices face the same risk of cyber-attack as any corporate computer system. Personal devices and apps downloaded to phones and tablets may be a threat to the IT network

Cybercrime and Cybersecurity risks:

- In 2018, cyber security experts observed 54% increase in new malware aimed specifically at mobile devices and blocked 24,000 malicious apps [i].
- 2018 statistics show that 2.958 billion people used their mobile device to access Facebook[ii], Twitter, and Instagram[iii]. A social network is ideal for cybercriminals to exploit, as malware spreads via connections between users.[iv]
- Complex software and apps often contain flaws[v] which can be exploited by cybercriminals. Vulnerabilities can exist in internet connected devices like fitness trackers, home security systems[vi], voice-activated virtual assistants[vii], and the apps that control them.

Benefits of Participation:

- Cyber security measures in the financial sector typically emphasise use of technological defences. There is a lack of research about users and risk.
- This study will focus on private use of personal technologies and identify unexplored risk which may be introduced when employees bring devices into the workplace.
- The aggregated findings will be shared with participating organisations to assist risk assessment and policy makers.

How to take part? All company personnel are invited to complete an electronic questionnaire (with industry standard privacy encryption) to survey personal use of technology. Taking approximately 12 minutes, the survey can be accessed via phone, tablet or computer.

The survey can be accessed at https://www.smartsurvey.co.uk/############
F**or more information, please contact:**

- r.collis@derby.ac.uk · Raichel Collis, PhD Researcher.
- d.hicks@derby.ac.uk · Dr David Hicks, Supervisor.
  MSc Criminal Investigation Programme Leader.

[1] Symantec (2018) *Internet Security Threat Report*. Volume 23. Available at: https://www.symantec.com/security-center/threat-report.
[1] https://www.statista.com/statistics/241462/global-mobile-phone-website-traffic-share/
[1] https://www.smartinsights.com/social-media-marketing/social-media-strategy/new-global-social-media-research/
[1] Sood, A. and Enbody, R. (2011) 'Chain Exploitation-Social Networks Malware', *ISACA Journal*, 1, pp.31-36. Available at: http://www.isacajournal-digital.org
[1] https://1902software.com/about/project/why-errors-happen-in-software-development/
[1] Spiezle, C. (2016) "Understanding the role of connected devices in recent Cyber-attacks". Available at: http://otalliance.actonsoftware.com/acton/attachment/6361/f-009d/1/-/-/-/-/House%20Statement%2011-15.pdfIoT
[1] https://www.cnet.com/news/security-researchers-warn-of-voice-vulnerabilities/

Appendix F: LinkedIn and Social Engineering

Introduction.

LinkedIn was used a search engine throughout the practical research in Chapters Four and Five (methodologies one and two). The site was instrumental in locating financial employees and identifying individuals by referencing personal information and visual images.

LinkedIn Profiles

Respondents were asked if they maintained a Linked-In profile and about the personal information they include on profile pages. Figure 47 (below) illustrates how respondents include at least one piece of personal information on their profile page. Sample size is thirty-one (N=31)

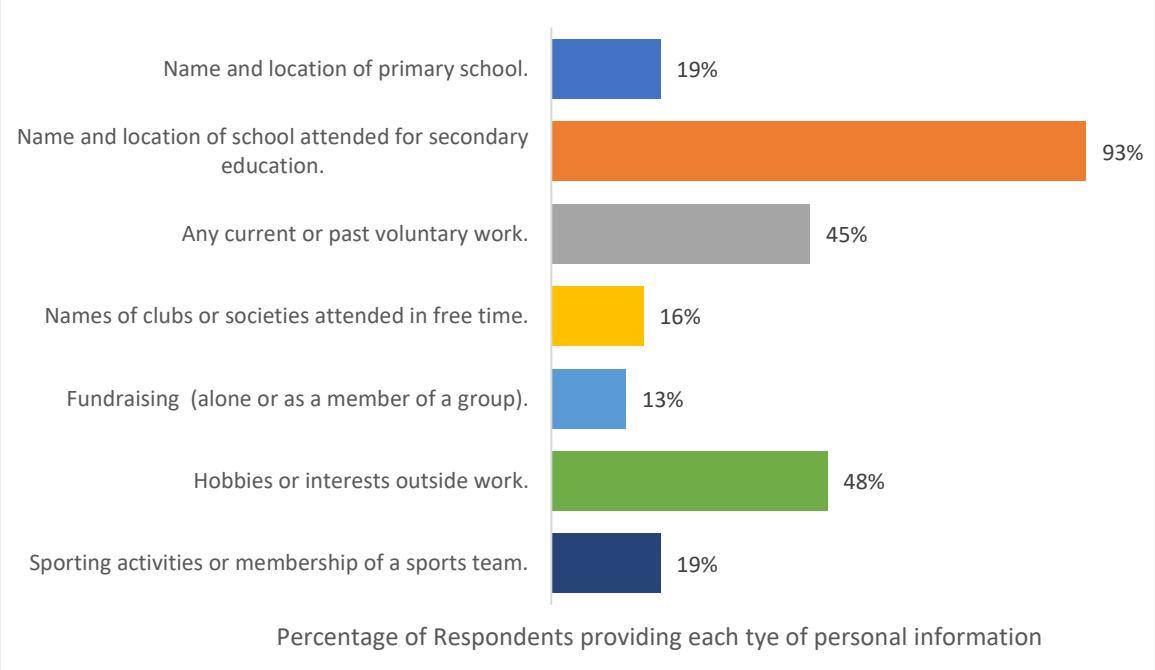

Figure 47. Type of Data on a LinkedIn Profile

For an attacker gathering intelligence the name and location of a secondary school can provide an indication of the geographical area where an individual

lived during the teenage years. This may then be used to search through media archives and news resources from that particular area. LinkedIn members often state post-graduate education on their profile pages, for example a master's degree or doctorate. It was observed during the open source research that individuals who returned to education as mature students typically attend a university in their local area. If secondary education took place in the same locality as the university attended for postgraduate study, the individual is likely to reside locally. The name of the town, city or district can then be used in conjunction with an individual's name when searching for social media accounts.

In the context of **RQ1 actual/perceived risks,** results were examined to see how many respondents made more than one piece of information available. Figure 48 (below) illustrates results.

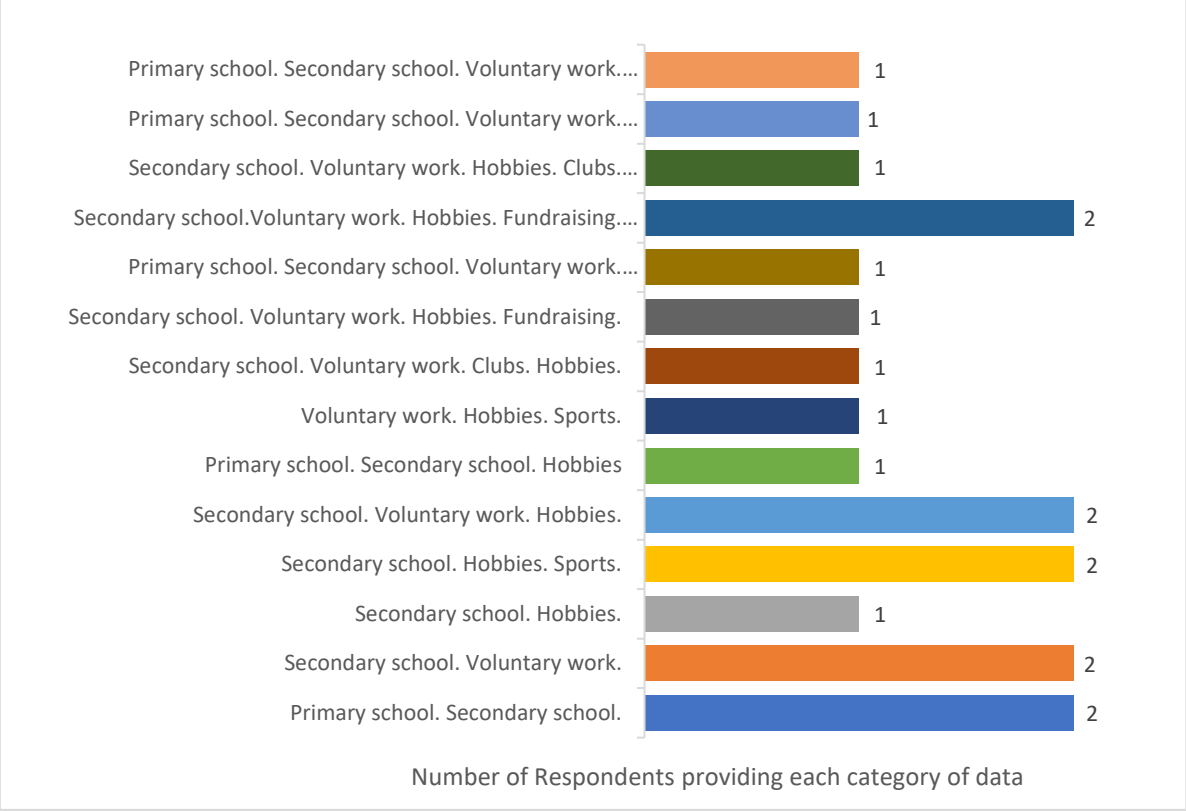

Figure 48. Personal Information on a LinkedIn Profile

Figure 48 illustrates how nineteen respondents placed sufficient information on their profiles for an interested party to begin to establish a comprehensive user profile. Fourteen respondents voluntarily placed three or more pieces of identifying data onto the internet, any of which may be used as keywords for dynamic searches in online databases or archives. LinkedIn is a business orientated site, with emphasis on networking and career enhancement and provides facility for users to apply for vacant positions. The site and is also utilised by recruiters who peruse profiles which have indicated they are open to new possibilities (No, 2019). It is understandable that LinkedIn members would choose to promote themselves favourably to other site members, nonetheless, users should be encouraged to think beyond building their 'personal brand' (Kunsman, 2018; Lake, 2019). Risk assessors and policy makers may be interested to learn how employees promote themselves on LinkedIn and recognise that information on the site may be used to make the corporation vulnerable. It is possible that the LinkedIn page of an employee would have been accessed during the recruitment process, since contemporary practice dictates that employers examine social media profiles when assessing suitability of candidates (Kohler, 2019). Nonetheless, content depicting skills and experience would likely have been the focus for a position in the financial sector, and personal data depicting hobbies and sports teams may have been overlooked. The results of the survey confirmed that participants were willing to admit to maintaining a LinkedIn profile, but when asked about the content, forty percent declined to respond. Hence, it may be prudent for risk assessors to examine the profiles of employees and suggest that non-essential data be anonymised or removed. This may have particular relevance due to a feature available to

LinkedIn users which prevents current employers and others in their network from that seeing that the user is open to new career possibilities (LinkedIn,2019). An employee hoping to attract the attention of a professional recruiter may provide so much information to boost their personal brand, that they become a potential liability.

Significance of LinkedIn to the Central Research Questions

Active use of social media, weak privacy controls, and an extensive network of associates all have relevance to **RQ1 actual/perceived risks** and in particular the identified risk of spear phishing as a high risk attack method. Thus, an employee with a comprehensive profile on LinkedIn may be a potential liability. This is especially relevant if it can be seen from the past and current employment that the individual is likely to have access to either critical corporate or customer data, or to be in a network or employment relationship with a key member of staff.

Employees who provide personal data on their profiles which can be used as fake credibility in phishing emails or other attack methods may be a risk to the corporation. As an example, several times during the open source research for this project, data on a LinkedIn profile page regarding primary education confirmed the identity of a subjects' extended family. This was achieved by conducting searches using a free online telephone directory as people of an older generation are more likely to have an active landline telephone. A search for the surname of the data subject in the geographical area named as the location for primary education found older parents who had either remained in the same town or village where they had raised their children or had moved to a nearby location.

Any search results were then included as search terms and the subjects social media accounts were used to confirm identification. This method confirmed identity of parents, grandparents, in-laws and often lead to the discovery of addresses and location of children's schools. In the context of **RQ1 actual/perceived risks** any data which convinces the recipient of a credible phishing attack may be thought of as a risk to the company.

Appendix G: Guest Networks

Introduction

The behaviours and activities of Group C who may threaten the corporate IT infrastructure were documented in 8.3 and 8.4 . Results showed that users undertook a variety of activities on devices which were later connected to the corporate network or possibly used to connect to other devices and share files and content. In accordance with **RQ2 average usage/impact**, harm might be introduced because of internet activity in the users personal space, or digital activity undertaken in the workplace. Nonetheless, the small sample of users who connect to the corporate network was surprising as it had been anticipated that more employees would use corporate facilities rather than their own mobile data plan.

During the survey, respondents were given a choice of 'yes', 'sometimes' and 'no' to answer the question asking if their device connected to the corporate network. No further enquiry was made of those who had responded negatively to ascertain whether their device gained internet access via alternative means. Only sixty-seven percent of respondents confirmed digital activity without corporate connectivity, thus thirty-three percent were either accessing the internet by alternate means or were not aware that their device had made an automatic connection to corporate WiFi.

Automatic Connection

Mobile devices (phones, tablets and laptops) that have previously connected to a

network will automatically remember it. Most devices offer the user the option to enable their device to re-connect to a known WiFi network when it is in range . (Ptsecurity, 2017) and the device will then connect seamlessly from one network to another, with limited intervention from the user. Respondent devices may be connecting automatically whenever in range of the corporate WiFi and as respondents are not manually enabling the connection, they may not realise the device is connected or indeed, even consider which network is providing their internet access. Users of some operating systems may not realise that their device will always select Wi-Fi ,even if mobile data is the preferred network (Grupé, 2019; Nagasamy,2019). Thus, without intending to use the corporate network, a user may be doing so inadvertently. If this is the case for some users in the sample, then the number of employees connected to the corporate network may be higher than illustrated. This may then be an issue for risk managers to consider as merely asking employees if their devices are connected to the network might not elicit an accurate result.

Guest Networks

If employees are not inadvertently connected to the network, they are achieving internet access via other means including personal mobile data or access to an alternative network. The failure to enquire about any alternate method of internet access is a limitation in the results, particularly if employees are using a network provided by their employer. Guest networks enable internet access for employees or visitors but prevent access to critical areas of the organisational network, for example sensitive corporate or customer data (Kaspersky, 2019b). Hence, the risk of sharing malware from a device compromised by personal internet activity

still exists. Other devices connected to the guest network and used for work purposes may be affected or a compromised device might share content or data to a device with access to the corporate network. In addition, a poorly configured guest network is a vulnerability which may allow internet harms to reach the crucial IT infrastructure (Rossi, 2015; Kaspersky, 2019b). Although recommended as a solution to safeguard corporate assets, security managers should still be aware that employee routine digital activity may still be a threat to corporate It infrastructure.

Appendix H: Cyber Awareness – Password Management

Introduction

Workplace Computers typically require a password to prevent unauthorised access and protect corporate and personal data. As more services move online, users have accounts with financial institutions, retail outlets, utilities and entertainment services, all requiring passwords to authorise a user as a legitimate owner. Subsequently, strong passwords managed competently is a fundamental requirement of basic cyber awareness and respondent attitude to password use has relevance to **RQ1 actual/perceived risks**. The survey contained two options associated with password use and respondents were invited to state how often they were likely to engage in particular behaviours.

Despite the availability of "password strength meters" (Li, Wang and Sun, 2017, p.1,) to encourage random characters and numbers, results confirm the literature by demonstrating that users prefer to use memorable data (ibid., 2017). The dataset was given an example of a child's name, a pet or date of birth and Figure 49 (below) illustrates how over half the respondents (fifty-four percent) stated they would 'Always', 'Quite Often' and 'Sometimes' create passwords using personal data. Sample size is seventy-two (N=72).

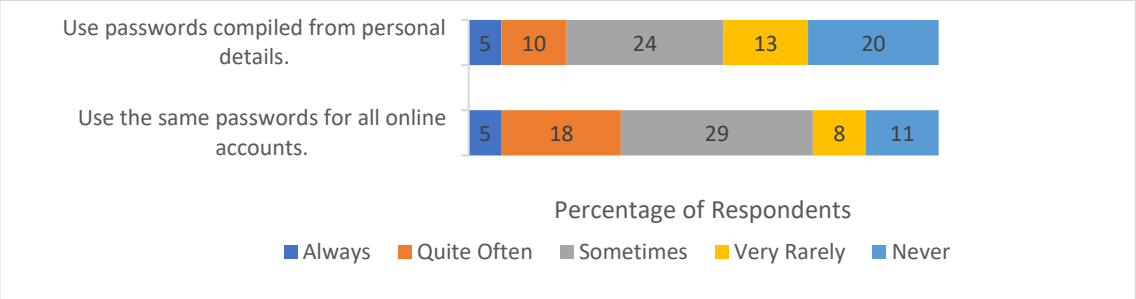

Figure 49. Passwords

From an offenders perspective, passwords using personal information are weak since data about a suitable target can be retrieved using internet resources, or by knowing the target personally (Li, Wang and Sun, 2017). In today's culture of social networking, gaining access to data by being friends on social media may equate to knowing someone personally (Li, Wang and Sun, 2017). In the context of **RQ1 actual/perceived risks**, an employee with an active social media presence who uses personal data in their passwords may be demonstrating poor cyber awareness.

Figure 50 illustrates data relating to how passwords were used. Sample size is seventy-one (N=71) and seventy-three percent indicated that they 'Always', 'Quite Often' and 'Sometimes' use the same passwords for all online accounts. If the same password is habitually used, then any easily deciphered password obtained by an attacker may grant access to other accounts and critical data. The limitations of these findings are that respondents were not specifically asked about work accounts nor passwords to corporate systems. Although a user may be lax in personal cyber habits yet demonstrate good awareness in the workplace, in respect to **RQ1 actual/perceived risks**, failings in password management may be an actual risk.

Appendix I: The NHS Cyber Attack

A contemporary example of the consequences of neglecting a security update is the WannaCry ransomware attack which took place in May 2017, affecting over two hundred thousand global users from one hundred and fifty countries (BBC, 2017). In the UK, thirty-four NHS trusts were *infected* by the WannaCry malware with a further thirty-six *affected* by the attack, causing severe disruption to healthcare services (Ghafur et al., 2019). Several weeks prior to the attack, Microsoft had issued an update to patch a known vulnerability in the Windows operating system. At the time, over ninety percent of NHS devices were using Windows 7, but the update did not take place. In addition, approximately five percent of health service IT equipment was still running Windows XP which Microsoft had ceased to support in 2015 (Morse, 2018).

The failure to update Windows 7 and the continued use of devices "running on legacy platforms" (Ghafur et al., 2019, p.6) enabled the malware to exploit the open vulnerability. After the attack, Microsoft issued a patch an unprecedented two years after withdrawing support for Windows XP, so that devices using the outdated system would be protected from further exploitation (Hanson, 2017). Investigation into the impact on the NHS highlighted a failure to respond to official advice. The Department of Health and the Cabinet Office had recommended that Trusts begin migrating from the outdated XP system before Microsoft withdrew support in 2015. Trusts had additionally neglected to apply the update for Windows 7, despite prompting from NHS Digital, the systems provider for health and social care (Morse, 2018). Alongside these faults, the official verdict was that

regardless of the failure to patch systems “taking action to manage their firewalls facing the internet would have guarded the organisations against infection” (Morse, 2018, p.16 para 2.4). This thus indicates that individual organisations had failed to maintain good cyber security practices including keeping anti -virus and firewalls updated (Morse, 2018, p.16, para 2.3).

The WannaCry attack was not targeted at the NHS organisations who became victims simply because they were connected to the internet using devices vulnerable to exploitation. The ransomware spread via the internet (Morse, 2018, p.11 para 1.2) yet three opportunities for potential guardianship were not enabled, resulting in routine activity allowing a convergence with an offender. Although the official reports did not allocate specific blame, it is likely that the decision not to enact the guardians was taken by users of devices and systems, possibly for the reasons of inconvenience stated in the grey literature. Risk assessors and policy makers may benefit from remembering that users may have their own motives for not keeping devices updated and thus should factor this into any risk assessments.

Confirmation of Ethical Approval

Kedleston Road, Derby

DE22 1GB, UK

T: +44 (0)1332 591060

E: researchoffice@derby.ac.uk

Sponsor License No: QGN14R294

Dear Raichel

Thank you for submitting your application to the College of Business, Law and Social Sciences Research Ethics Committee, which has now been reviewed and considered.

The outcome of your application is: approved.

If any changes to the study described in the application are necessary, you must notify the Committee and may be required to make a resubmission of the application.

On behalf of the Committee, we wish you the best of luck with your study.

Yours sincerely

Christopher James

Request for Ethical Approval for Research

Your Name	**Raichel Collis**
College	**BLSS**
College Research Ethics Committee	**BLSS**
Staff ID	
Student ID	**002545758**
Unimail address	**r.collis@ derby.ac.uk**
Programme name / code	**PhD**
Name of supervisor(s)	**Dr D Hicks, Dr Philip Hodgson, Professor Alex Nunn**
Title of proposed research study	
(Mis)-Use of Personal Technologies by Financial Sector Employees	
Background information	
Has this research been funded by an external organisation (e.g. a research council or public	**no**

sector body) or internally (such as the RLTF fund)? If yes, please provide details.	
Have you submitted previous requests for ethical approval to the Committee that relate to this research project? If yes please provide details.	**Yes** **This ethics application was approved by the LHSS-CREC on 8 March 2017, and research has been conducted under DPA 1998.** **The application is being re-submitted for ethics approval relating to the questionnaire (still to be conducted) as well as compliance with the General Data Protection Regulation (GDPR) and Data Protection Act 2018. Amended and additional text to the 2017 submission are noted below in coloured font, and with strikethrough to indicate items that are no longer applicable.**

Are other research partners involved in the proposed research? If yes please provide details.	**No**

Signatures

The information supplied is, to the best of my knowledge and belief, accurate. I clearly understand my obligations and the rights of the participants. I agree to act at all times in accordance with University of Derby Policy and Code of Practice on Research Ethics: http://www.derby.ac.uk/research/uod/ethics/

Signature of applicant	**Raichel Collis**
Date of submission by applicant	**2 November 2016 19 November 2018**
Signature of supervisor (if applicable)	**Copyright content removed**
Date of signature by supervisor (if applicable)	**19 November 2018**

For Committee Use ***Reference Number (Subject area initials/year/ID number)***

……

Date received …….. **Date considered**

……

Committee decision …….. Signed ……

Ethics ETH1819-0032: Ms Raichel Collis

Date Created **19 Nov 2018**

Date Submitted **19 Nov 2018**

Date of last resubmission **23 Nov 2018**

Date forwarded to **19 Nov 2018 committee**

Researcher **Ms Raichel Collis**

Student ID **002545758**

Category **Postgraduate research student**

Supervisor **David Hicks**

Project **Doctoral Research Project**

College **College of Business, Law and Social Sciences**

Current status **Approved**

Ethics application

Initial screening

Does the project involve collecting and/or analysing primary or unpublished data from, or about, living human beings? Yes

Does it involve collecting or analysing primary or unpublished data about people who have recently died, other than data that is already in the public domain?

No

Does it involve collecting or analysing primary or unpublished data about or from organisations or agencies of any kind, other than data that are already in the public domain? Yes

Does it involve research with non-human vertebrates in their natural settings or behavioural work involving invertebrate species not covered by the Animals Scientific Procedures Act (1993)? No

Does this project involve human participants? Yes

Background

Title of current research study

(Mis)Use of Personal Technology by Employees in Financial Services Organisations

Has this research been funded by an external organisation (e.g. a research council or public sector body)?

No

If yes, please provide the name of funder:

Has this research been funded internally (such as the RLTF fund)?

No

Have you submitted previous requests for ethical approval to the Committee that relate to this research project? Yes

Was the title of research study the same on previous applications for approval?

No

If no, title of previous application and Ethics Application ID if available:

(In)Appropriate Cyber Behaviour and Risks to Financial Organisations

Date previous application for approval was submitted

02 Nov 2016

Was the previous application approved? Yes

Are other research partners involved in the proposed research?

No

If yes, please provide details

Should your research adhere to the British Psychology Society (BPS) code of ethics and conduct? No

Study

What is the aim of your study? What are the objectives for your study? aim of study

To identify whether employees within financial organisation(s) are unknowingly engaging in (in)appropriate cyber behaviour and exacerbating the risk of cyber - crime against the corporate IT network.

To help financial corporations understand that cybercrime is not merely a technological issue and aid in understanding the actual rather than the perceived risk posed by personnel within the workplace.

To help financial institutions comprehend how users make use of their own mobile devices and how this may impact upon the corporate IT infrastructure.

To assess whether devices and applications associated with the Internet of Things (IoT) are finding a presence within the workspace and evaluate the potential risks they may entail.

Brief review of relevant literature and rationale for study

The threat of cyber-attack to United Kingdom (UK) industry and infrastructure has been identified as a key issue to be addressed and as such, a comprehensive range of cyber security measures have been put in place (HM Government 2015, Cabinet Office 2016).

The Bank of England (BoE) has acknowledged cyber-attack as “a serious and growing threat” faced by the UK financial industry (BoE, 2015 p.14) and have introduced the CBEST (this is not an acronym with underlying words but rather, as confirmed by the BoE, a brand for recognition purposes) system of bespoke threat intelligence and penetration testing to assess resilience and identify weakness within the IT infrastructure of a financial institution. However, despite recognising that employees within an institution should be considered as a potential resource to be exploited by a threat actor (BoE, 2016c), the apparent emphasis for cyber security is predominantly on technological solutions (BoE,2016, Salim and Madnik 2014.

Annual reports published by the cyber security sector continue to identify successful data breaches and cyber- attacks where human end-users have played a key role in allowing the attacker to access the network (Verizon, 2015 p.14, Symantec, 2015, p.79). It is possible that average users of technology (those without specialist IT skills or niche training) may be unknowingly engaging in (in)appropriate cyber behaviour either within the workplace or outside the work environment. Factors may be ignorance and lack of proficiency, indifference to risk associated with technology or a frustration with corporate hierarchy causing competent, but impatient users to source their own solutions to technological problems.

Academic literature explores the culture of BYOD (Bring Your Own Device) within corporations and suggests security remedies (Zahadat et al., 2015) in addition, the threat of malicious insider activity and social engineering has been investigated (Punithavathani, et al 2014; Silic and Back 2016; Mouton et al 2016).

However, in order to gain a greater insight into the potential cyber risk within an organisation, a comprehensive evaluation of all personnel entering the workspace should be undertaken. This should ideally include all employees, visitors, guests and contractors, and focus in particular on technological competency, cyber awareness and the internet connectable mobile devices (smartphones, tablets, laptops) which are brought into the workspace for work and/or personal use which may be unknowingly connected to the corporate IT network.

BYOD is permitted within many institutions as an addition to the working environment and a method of reducing company costs (Walker-Osborn et al,2013; Utter and Rea 2015). Additionally, as 81% of UK adults now possess a smartphone (Daly, 2016) it must be considered that internet connectable devices may be entering the workspace in bags, pockets or vehicles which may park close enough to the premises to access the network. (Organisations may have procedures in place to mitigate security threats created by mobile devices (Rivera et al., 2013) however, technology is rapidly evolving, new platforms of online communication are embraced by users and the use made of mobile devices by private owners; including gambling, social networking, social discovery, streaming, gaming, adult websites, content sharing etc. may be introducing unidentified and unexpected security issues into the workspace.

Anti-virus software and applications may slow or impede the operating system of a phone or tablet, therefore privately owned devices can introduce risk as users may neglect security precautions (Symantec, 2015, p.8) or avoid antivirus solutions (Chen et al 2015 p.194). However, both Android and Apple (iOS) operating systems are vulnerable to applications (apps) which can include

malicious software (malware) “in disguise” (Symantec, 2015 p.8) remote attacks (Verizon,2015, p.19) and En Public apps capable of hijacking a genuine iOS application (Verizon, 2015, p.19). Malware designed to infect mobile devices can be introduced via Bluetooth (Symantec, 2015 p.19), text message (Symantec, 2015p.25) email and social media and can then propagate to other devices after infection (Chen et al, 2015).

may be inadvertently introducing vulnerabilities into the IT Infrastructure via downloaded or shared content, free or open source software and apps supported by their device. A device not connected to the network can still be vulnerable as malware can spread via sharing of files including work documents or personal files (music, video etc.). Even a device carried on site within a bag or pocket can be susceptible to sophisticated malicious code if the Bluetooth system is activated (Paullet and Pinchot, 2014, Jackson and Creese, 2012).

An emerging risk to corporations has appeared as the Internet of Things (IoT) has evolved and smart devices aimed at consumers are becoming common. Already established within healthcare, manufacturing, retail, logistics and building management, IoT devices can monitor environmental controls, stock levels or security cameras using the internet to connect and share data. The connected systems learn and recognise patterns from information gathered via sensors embedded in devices and machines. An example within a ‘smart’ building is the use of sensors to track locations and movements of the occupants, analyse how space within the building is being utilised and then automatically adjust ventilation and lighting accordingly (Roth, 2016). However, smart gadgets and appliances aimed at the home user are currently becoming popular. Ernst and Young predict

that over fifty billion smart units will be connected by 2020 (EY, 2015, p.1) including coffee percolators, fridges (Storey, 2014, p.9), robotic hoovers, pet monitoring cameras and wearable health monitors (EY,2015 p.4), Also home heating and lighting systems. Such devices and gadgets can be controlled from any location (Hewlett Packard, 2015, p.3) via an app which must be downloaded to a smartphone or tablet. As IoT devices are connected to the internet, they are vulnerable to typical internet threats, for example, “malicious code hacking attacks” (Vermesan and Friess, 2014 p.91). Corman (interview with Hewlett Packard Enterprises, 2016) implies that it is not inconceivable for an attacker to hack into an organisation via the office coffee maker or a wearable fitness tracker, suggesting that any device using software should be thought of as ‘hackable’ and if internet connected, should be considered to be ‘exposed’. A further security risk to consider is that if applications downloaded to phones or tablets have no secure connection to the cloud infrastructure supporting the device they control (Barcena and Wueest,2015), it is that mobile devices entering the workspace could introduce a new threat to the corporate network.

Academic literature pertaining to computers and the internet, tends to be technological in nature, aimed at those with an understanding of computer science or IT networks and typically offers new solutions and frameworks for security and code development. If discussing the human element, the literature addresses insider threat (Agrafiotis et al., 2015), the necessity for more robust cyber security training for staff (Salim and Madnick, 2014) or the danger that end-users perceive for themselves regarding their online safety or internet use (Byrne et al., 2016; Tsai et al., 2016).

The primary focus of this investigation will be the average end-users of contemporary technologies and will concentrate upon human behaviour with the internet, digital content and devices utilised in and out of the workplace. Exploring the potential for harm created by the development of consumer IoT and a greater understanding of actual, rather than perceived risk posed by the personnel within an organisation will provide new insight into the human dimension behind successful cyber-attacks. Thus, this research has the potential to provide more comprehensive cyber risk management strategies for financial corporations.

Outline of study design and methods

The purpose of this study is to identify whether average users of technology (those without specialist skills or niche IT training), are enabling access by cyber criminals due to (in)appropriate actions and activities using the internet. Users may be unknowingly abetting internet crime through lack of awareness, ignorance of technology and/or inappropriate cyber behaviour, exacerbated by the personal use of mobile devices which are then brought into the workplace and granted access to the corporate IT network.

There are three methods proposed to recruit the sample.

Method 1. Independent Financial Services Organisations in Derby

Letters of introduction will be sent to independent financial organisations in the local Derby area, with a request that the organisation consider participating in the project. The organisations will be located by examining internet resources where local businesses are indexed, directories listing local enterprise by sector and keyword search techniques. Small and medium sized organisations with a team of

staff and an active website will be approached. The website is relevant as independent organisations typically provide online profiles of their employees on the corporate webspace. It will therefore be possible to ascertain who the letter of introduction should be addressed to. In small organisations, the company director may also act as secretary and thus be the person who should receive the letter. In larger organisations , a director of operations may have responsibility for guiding post to the appropriate recipient.

Only organisations based in Derby City or the local area will be approached. The letter of introduction will be printed onto a University letter -head and it is hoped that organisations may see benefit in collaborating with the local university. Independent organisations will be selected as they are more likely to have autonomy over internal decision-making than those affiliated with large corporations. Small businesses may be vulnerable to incidents of cybercrime, due to lack of resources or knowledge regarding cyber security (Ling, 2018). Hence independent organisations who recognise value in the research are in a position to make a prompt decision about taking part. Large corporations governed by seniors based at a remote head office may be restricted by a hierarchy of management.

The methods already used in this project (See original ethics application)indicate that if a recipient is interested and wishes to know more about the study, they will respond promptly by email and request further information via a telephone conversation. This prior knowledge is helpful for estimating timescales. The introductory letter includes the link to the electronic survey but also offers the option for an interested recipient to request more information by email, thus it is

probable that letters posted in the last week of November will elicit either a telephone conversation or survey responses by or within the first week of December. This is important as the Christmas period is typically busy, particularly for small enterprise and it is preferable that the introductory letter not be lost amongst an increase in postal items.

It is anticipated that any organisation interested in participating will access the GDPR compliant research instrument in the first week of December. This will allow sufficient time for employees to volunteer before the Christmas period commences.

Method 2. Personal Connections

Colleagues who have personal or professional connections to financial corporations will be asked for personal introductions. A personalised letter of introduction will be sent to the appropriate person, followed by a telephone conversation. Personal acquaintances who work in financial services will be asked to complete the GDPR compliant research instrument. The electronic survey can only be accessed via a web link, so no email address is collected, and the survey has been configured to not collect a respondents IP address. Respondent privacy is protected by use of industry standard encryption methods and the questions do not ask for any personal information thus affording anonymity to employees and organisations.

Method 3. Participation of large Financial Organisations.

The methods already used in this project elicited a response from a large financial organisation who expressed interest in the research study but could not commit to

participate due to pressure of work and time. The organisation’s representative will be approached again with the GDPR revised documents.

Please provide a detailed description of the study sample, covering recruitment, selection, number, age and if appropriate, inclusion and exclusion criteria.

The research will focus on the financial sector due to the high volume of technological systems in place and the need for high-level cyber security (Bank of England 2015, BoE 2016). For the purposes of this study, the financial industry can be considered to be any professional service engaged in the management of money, for example, accounting, banking, insurance, pensions, credit cards etc.

The intention is to survey personnel working within the financial sector, to assess levels of technological competence, cyber awareness, individual internet practices and personal usage of mobile devices. Therefore, the sample will consist of individuals employed in any capacity, who may be based within a corporate office building or may be employed by a third party and enter an organisation's premises as a requirement of their employment.

Occupations could potentially range (as an example) from senior account management to catering or cleaning. Hence, the criteria for inclusion in the study is that the participant must physically or remotely access a financial corporation workspace (an office, business premises, virtual desktop etc.), own or utilise a mobile device (smartphone, tablet, laptop, netbook etc.) and must be aged eighteen or over.

Are payments or rewards/incentives going to be made to the participants?

No

If yes, please provide details

Do you intend to give participant points for taking part in your study?

No

What resources will you require?

As a complex questionnaire is required, utilising advanced survey logic and incorporating filtering, skip logic, and piped answers to build a framework for progressive questioning, an online survey package offering premium services to paid subscribers has been purchased by the researcher. A premium service will allow greater flexibility and creativity when designing the questionnaire and University of Derby branding can be added, thus aiding with credibility for the researcher. Smart Survey (available at https://www.smartsurvey.co.uk) offers all the features required to create a superior survey experience.

The sophisticated electronic survey will collect both quantitative and qualitative data incorporating Likert scales and open questions to provide the option for additional comments. The software package will filter out any non-relevant participants and responses will be piped from previous questions to ensure only pertinent questions.

Some questions have been removed from the original questionnaire presented to the research ethics committee, approved in March 2017. Other questions have been amended and new ones added to reflect changes in contemporary technologies. Despite containing fifty-eight questions, the sample questionnaire

has been simplified to enable it to be inserted into this document. The electronic survey contains seventy-six questions overall but contains survey logic ensuring that each participant takes an individual pathway through the questionnaire, dependent on personal responses. As such, a respondent will typically answer approximately thirty questions. The survey is accessed via a weblink which takes the participant directly to the landing page (the first page viewed by a respondent when accessing the survey) where the privacy notice and the consent sheet must be viewed before the questionnaire can be accessed. Unless the respondent provides explicit consent to continue, the questionnaire will not load onscreen. Thus, a respondent who withholds consent will be taken to the debrief document and the survey is over. A respondent also has the option to leave the survey at any time by closing their web browser. The participant information sheet will be on the first screen to appear after the link to the survey has been opened. For ease of use, it will be combined with the consent form.

In order for participants to monitor their route through the survey, ‘progress’ and ‘time remaining’ indicators will be visible on each screen.

Questions will relate to mobile device use in and out of the workplace, technological expertise and internet use /cyber awareness. At regular intervals, it will be reiterated that all data is anonymous, and the respondent will be encouraged to enter candid and open responses.

Using survey logic, relevant respondents will be diverted to a further short questionnaire about Internet of Things devices, wearables and apps.

The final screen will be a debrief document which will load after the final question and will offer the candidate the option to submit the survey or exit. The survey will be generic, regardless of whether it is sent an individual or to an organisation.

References for any sources cited in the sections on rationale, methods etc.

Agrafiotis, I., Nurse, J.R., Buckley, O., Legg, P., Creese, S. and Goldsmith, M. (2015b) 'Identifying attack patterns for insider threat detection', Computer Fraud & Security, 2015(7), pp. 9–17. Bank of England, 2015. Financial Stability Report [Pdf] Available at http://www.bankof england.co.uk/publications/Documents/fsr/2015/fsrfull1507.pdf [Accessed 12 December 2015] Bank of England (2016) CBEST intelligence-led testing an introduction to Cyber Threat Modelling version 2.0. [Pdf]Available at: http://www.bankofengland.co.uk/Financiastability

/fca/Documents/anintroductiontocbest.pdf [Accessed 13 June 2016]

Bank of England (2016c) CBEST Implementation Guide. [Pdf] Available at:

https://www.bankofengland.co.uk/financialstability/fsc/.../cbestimplementationguide.pdf. [Accessed 24 June 2016]

Barcena, M.B. and Wueest, B.C. (2015) Insecurity in the Internet of Things. Available at:

https://www.symantec.com/content/en/us/enterprise/fact_sheets/b-insecurity-in-the-internet-of-thingsds.pdf [Accessed: 3 July 2016]

Byrne, Z.S., Dvorak, K.J., Peters, J.M., Ray, I., Howe, A. and Sanchez, D. (2016) From the user's perspective: Perceptions of risk relative to benefit associated with using the Internet, Computers in Human Behavior, 59, pp. 456–468.

Cabinet Office (2016) The UK Cyber Security Strategy Annual Report 2011 - 2016. [online] Available at: https://www.gov.uk/.../UK_Cyber_Security_Strategy_Annual_Report

2016.pdf [Accessed13 June 2016].

Chen, P.S., Lin, S.-C. and Sun, C.-H. (2015) 'Simple and effective method for detecting abnormal internet behaviours of mobile devices', Information Sciences, 321, pp. 193–204.

COP Guidance (2013) Research guidance note 4 Online Survey tools. Available at: http://staff.napier.ac.uk/services/research-innovation-office/policies/Documents/Integrity/ COPguidance4.pdf (Accessed: 17 May 2016).

Coulson, N. (2015) Online Research Methods for Psychologists. United Kingdom: Palgrave Macmillan.

Daly, R. (2016) There's no place like phone consumer usage patterns in the era of peak smartphone. Available at: http://www.deloitte.co.uk/mobileuk/assets/pdf/Deloitte-Mobile-Consumer-2016-There-isno-place-like-phone.pdf [Accessed: 4 October 2016].

Ernst & Young Global Ltd (2015) Cybersecurity and the Internet of things insights on governance, risk and compliance. [pdf] Available at :<http://www.ey.com/Publication/vwLUAssets/EYcybersecurity-and-the-internet-of-

things/$FILE/EY-cybersecurity-and-the-internet-of-things.pdf [Accessed: 18 December 2015]

Hewlett Packard Enterprise (2015) Internet of Things Research study: 2015 report [[Pdf]. Available at: http://h20195.www2.hp.com/V2/GetDocument.aspx?docname=4AA5-4759ENW&cc=us&lc=en [Accessed: 24 January 2016].

Hewlett Packard Enterprise (2016) *Josh Corman leads the drive to make 'smart' devices secure – HPE business insights.* Available at: https://www.hpe.com/h30683/us/en/strategic-businessinsights/c/enterprise-security/innovation/josh-corman-leads-the-drive-to-make--smart--devicessecure.html [Accessed: 7 October 2016].

HM Government (2015) *National Security Strategy and Strategic Defence Review 2015*. Available at: https://www.gov.uk/.../system/.../52309_Cm_9161_

NSS_SD_Review_web_only.pdf. [Accessed 20 June 2016]

Jackson, J, & Creese, S 2012, 'Virus Propagation in Heterogeneous Bluetooth Networks with Human Behaviours', IEEE Transactions On Dependable & Secure Computing, 9, 6, p. 930, Publisher

Provided Full Text Searching File, EBSCOhost, [Accessed 2 July 2016]

Ling, J. (2018. The human factor: why behaviour is the weak link in cybersecurity - Security News Desk. Available at: http://www.securitynewsdesk.com/human-factor-behaviour-weak-linkcybersecurity/ [Accessed 15 November 2018].

Markham, A. and Buchanan, E. (2012) FINAL DRAFT: Ethical Decision-Making and Internet Research: version 2.0. Recommendations from the AOIR Ethics Committee. [Pdf] Available at: http://aoir.org/reports/ethics2.pdf> [Accessed 9 September 2016]

Mouton, F., Leenen, L. and Venter, H.S. (2016) 'Social engineering attack examples, templates and scenarios', Computers & Security, 59, pp. 186–209.

Paullet, K., Pinchot, J. (2014) Mobile Malware: Coming to a smartphone near you, Issues in Information Systems, 15(2), pp. 116–123.

Punithavathani, D.S., Sujatha, K. and Jain, J.M. (2014) Surveillance of anomaly and misuse in critical networks to counter insider threats using computational intelligence, Cluster Computing, 18(1), pp.

435–451.

Rivera, D., George, G., Peter, P., Muralidharan, S. and Khanum, S. (2013) Analysis of security controls for BYOD (bring your own device). [online] Available at: http://hdl.handle.net/11343/33338 [Accessed: 2 July 2016].

Roth, I. (2016) Smart sensors at the forefront of building intelligence | smart buildings. Available at:

http://www.smartbuildingsmagazine.com/features/smart-sensors-at-the-forefront-of-buildingintelligence [Accessed: 5 October 2016].

Salim, H.M. and Madnick, S.E. (2014) Cyber safety: A systems thinking and systems theory approach to managing Cyber security risks. Available at: http://ic3.mit.edu/ResearchSamples/2014-

12.pdf [Accessed: 3 October 2016].

Silic, M.and Back, A. (2016) The dark side of social networking sites: Understanding phishing risks, Computers in Human Behaviour, 60, pp. 35–43.

Storey, A. (2014) 'There's nothing "smart" about insecure connected devices', Network Security, 2014(7), pp. 9–12.

Symantec, (2015) Internet Security Threat Report. [Pdf] Available at:

https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347932_GA-internet-security-threat-reportvolume-20-2015-social_v2.pdf [Accessed 12 December 2015]

The Survey Unit, (2013) Surveys: Frequently Asked Questions. Available at: http://www.nottingham.ac.uk/survey-unit/surveyFAQs.htm#top [Accessed 31 October 2016]

Tsai, H.S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N.J. and Cotten, S.R. (2016) 'Understanding online safety behaviors: A protection motivation theory perspective', Computers & Security, 59, pp.

138–150. doi: 10.1016/j.cose.2016.02.009.

Utter, C.J., Rea, A. (2015) The "Bring Your Own Device" conundrum for organisations and investigators: An examination of the policy and legal concerns in light of investigatory challenges.

The Journal of Digital Forensics, Security and Law 10(2), pp. 55-71.

Verizon (2015) RP Data Breach Investigation Report 2015 [Pdf] Available at: http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigationreport_2015_en_xg.pdf [Accessed: 3 July 2016].

Vermesan, O. and Friess, P. (Eds) (2014) Internet of Things – from research and innovation to market deployment. River Publishers series in communication. [online] Available at: http://www.internet-of-things-research.eu/pdf/IoT-From%20Research% 20and%20Innovation%20to%20Market%20Deployment_IERC_Cluster_eBook

_978-87-93102-95-8_P.pdf [Accessed: 3 July 2016].

Walker-Osborn, C. Mann, S., and Mann, V. (2013) 'to Byod or … not to Byod', Itnow, 55, 1, p. 38,

Publisher Provided Full Text Searching File, EBSCOhost, [Accessed 2 July 2016]

Zahadat, N., Blessner, P., Blackburn, T. and Olson, B.A. (2015) BYOD security engineering: A framework and its analysis, Computers & Security, 55, pp. 81, 99.

Ethical considerations

Consent

Respondents who volunteer to access the electronic survey have the option to complete it on any device (phone, tablet or computer). Hence, the survey has been formatted so that all information will be displayed clearly, regardless of the shape of the user's screen. The landing page will therefore display all the necessary information concerning privacy and consent. The page begins with the purpose of the study and explains that the reason the respondent has been invited to participate is because they are a member of personnel at a financial services organisation. This is followed by the privacy notice.

The privacy notice will precede the consent sheet and participants must scroll and read through it in order to reach the consent buttons. The privacy notice informs that privacy is protected by UK/EU industry standard encryption and all data provided will be held and processed in compliance with the Data Protection Act 2018, the General Data Protection Regulation (GDPR) and subsequent legislation. Respondents are informed of the data protection credentials held by the survey provider who is compliant with GDPR data collection requirements, uses UK/EU based servers and is certified to internationally recognised standards for information security management (ISMS). The lawful basis for data collection is explained alongside the target date for securely destroying the data on completion of the project.

The privacy notice provides respondents with the name and contact email for the researcher and informed that the data is being collected for PhD research with the University of Derby. The right to withdraw is explained, along with the process for enabling withdrawal and the process to complete it within a specific time scale. Respondents are additionally advised that as data subjects they may contact the

university Data Protection Officer and request withdrawal, thus suitable contact details are also provided. Below the privacy notice, the page displays two radio buttons where the recipient can either confirm or deny explicit consent. If the participant confirms consent, the next page of the survey will load, and the questionnaire will begin. If no consent is indicated, the survey ends immediately, and the participant is taken to the debrief page where they may leave the survey. The consent page has been configured to require an answer, to prevent the page being 'skipped'. Attempting to leave the page without answering the question will result an error message being displayed. Hence, without confirmation of explicit consent, the respondent cannot continue to the questionnaire. The consent page additionally provides a data field to create a unique identifier so that an individual can be identified in case of any request to withdraw. This is explained further in part d.

Withdrawal from the Investigation.

When the respondent reaches the final page of the survey, they are again asked to confirm explicit consent to submit their data. The second consent page has also been configured to require an answer, so the respondent cannot 'skip' the question. If consent is confirmed, the respondent will be taken to the page where the survey can be submitted. If the respondent chooses to withhold consent, the survey will end and the debrief page will load. Without confirmation of explicit consent, the respondent cannot submit the survey.

As the privacy notice and consent are combined into one page on the electronic survey, the appendices for this application have been arranged as a representation of what a respondent will experience when they access the survey.

Hence the attachment accompanying this application includes the privacy notice and the consent sheet formatted as they will appear on-screen.

Deception

the researcher intends to approach organisations/entities in her own name and GDPR /Data protection compliance has been addressed.

Debriefing

The debrief document will load onto the final screen after the respondent has completed the survey. The page explains the purpose of the study, informs that the project was granted ethical approval and includes contact details for the researcher so that the respondent may ask further questions or request a copy of the aggregated findings. If a respondent has any concerns about the project, contact details for the Director of Studies are also included. The process for withdrawal is explained, along with an explanation of the reason for a limited withdrawal period. The document reiterates the information provided in the privacy notice and informs respondents that data will be held and processed in compliance with the Data Protection Act 2018, the General Data Protection Regulation (GDPR) and subsequent legislation. As the researcher is not qualified to offer advice, respondents are signposted towards suitable resources concerning cyber awareness, internet safety and the Action Fraud cybercrime reporting centre. A link to the Information Commissioner's Office (ICO) website is included, so that respondents can learn more about data protection and their rights as data subjects. Respondents are additionally suppled with contact details for the Data Protection Officer and Deputy DPO at University of Derby.

Withdrawal from the investigation

The research instrument is accessed directly via a web link so cannot retain any email addresses, and none of the questions request any personal data from respondents. In addition, the survey software has been configured so that no IP addresses are collected and the option to ‘save and continue’ has been disabled as offering this option would require the use of respondent email addresses. As respondents are therefore anonymous to the researcher, in order to offer the right to withdraw, the privacy notice advises the respondent to create a unique identifier (not using dates of birth nor names) and to’ retain it. If a respondent wishes to withdraw, the unique identifier and the word ‘withdraw should be used as the subject heading in an email the researcher, who will consequently remove their data from the investigation. A capture field has been inserted into the landing page of the survey directly below the consent button, and the respondent is advised to create a six-figure code of three letters and three numbers. Clear instructions are displayed regarding the withdrawal procedure, the requirement to create and retain a code alongside the researchers email address for respondents to use if necessary.

The debrief document has the option to be printed for the responded to retain, therefore it reminds the respondent of the right to withdraw and repeats the process and contact details for the researcher. The debrief additionally contains the contact details for the Data Protection Officer at University of Derby, should the respondent wish to exercise their rights as a data subject and withdraw from the study.

Withdrawal Timescale

When the letters of introduction are posted to named people in organisations, the survey will be opened to collect responses. Although the time scale for organisations to respond cannot be certain, it is probable that if an organisation is interested in participating, the survey will be accessed during the first two weeks of December 2018. The survey will likely remain open until Friday 21st December 2018. Results are collected and stored electronically thus the date of submission can be observed. After fourteen days, if no request to withdraw is received the data will be aggregated for analytical purposes**.**

Confidentiality

The electronic survey has been configured to prevent collection of any personal data including IP addresses and email addresses. The questionnaire does not ask for any personal data other than gender, age, nationality, level of education, position in company (not job title) and whether full-time or part-time employee.

All information provided will be held and processed in compliance with the Data Protection Act 2018, the General Data Protection Regulation (GDPR) and subsequent legislation. Respondent privacy is protected by UK/EU industry standard SSL (Secure Socket Layer) encryption. The survey provider is compliant with GDPR data collection requirements, uses UK/EU based servers and is certified to internationally recognised standards for information security management (ISMS).

Only aggregated, analysed findings will be offered to participating organisations at the conclusion of the study and associated academic work. Any comments quoted

within the findings will be given pseudonyms, therefore individuals will always remain anonymous and their data confidential.

Protection of participants

Participation in this research study is entirely voluntary. Organisations and individuals are at liberty to request information about the study before deciding to participate and accept or decline the invitation as they see fit. Respondents can withdraw at any time during the electronic survey and up to 14 days after submitting the survey. The survey has been configured and designed to protect respondent privacy and uses UK/EU industry standard SSL (Secure Socket Layer) encryption

All information provided will be held and processed in compliance with the Data Protection Act 2018, the General Data Protection Regulation (GDPR) and subsequent legislation. The survey provider is compliant with GDPR data collection requirements, uses UK/EU based servers and is certified to internationally recognised standards for information security management (ISMS).

Observation research

not applicable to this research study.

Giving advice

The researcher is not qualified to offer advice; therefore, respondents are signposted towards suitable resources concerning cyber awareness, internet safety and the Action Fraud cybercrime reporting centre. A link to the Information Commissioner's Office (ICO) website is included, so that respondents can learn

more about data protection and their rights as data subjects. Respondents are additionally suppled with contact details for the Data Protection Officer and Deputy DPO at University of Derby**.**

Research undertaken in public places not applicable to this research study.

Data Protection (GDPR considerations)

This application for ethical approval is to ensure the online questionnaire and associated documents comply with Data Protection considerations.

Respondents are notified that the information they supply will be processed in accordance to the Data Protection Act 2018, GDPR and subsequent legislation.

Respondents are informed of the name of the student researcher and the legal basis for collecting the information.

Respondents are informed how long the information will be held for and the date it will be securely destroyed.

Respondents are asked to give explicit consent for their data to be used as stipulated.

Animal Rights

not applicable to this research study.

Environmental protection not applicable to this research study.

Are there other ethical implications that are additional to this list?

No

If yes, please provide details

Have/do you intend to request ethical approval from any other body/organisation?

No

If yes, please provide details

Do you intend to publish your research? Yes

If yes, what are your publication plans?

Unknown at this time

Have you secured access and permissions to use any resources that you may require? No

If yes, please provide details

Have the activities associated with this research project been risk-assessed?

Yes

If yes, please provide details

Risk assessment took place at the RD5 stage, submitted 24 February 2016

Attachments

Cover letter/invitation to participants

Information sheet about your research study

Focus group questions

Self-completion questionnaire

Debriefing material

Location consent form

Psychometric scales

Interview questions/schedules

Informed consent forms for participants

Informed consent from other parties/organisations

Relevant testing materials

Other

This application for ethical approval is for Data Protection /GDPR compliance for the online questionnaire and associated documents. Please refer to the file Collis-Criminology PhD Research which is the original ethics application approved by the LHSS-CREC on 8 March 2017. This document incorporates all Data Protection /GDPR amendments in the context of the research conducted under DPA 1998.

Included files

1. **Privacy Notice incorporating consent (formatted as it appears on-screen to participants).**
2. **Self-completion questionnaire.**
3. **Debrief Document (formatted as it appears on-screen to participants).**

(Letter of Invitation is available in Appendix E)

1. Privacy Notice Incorporating Consent (formatted as it appears onscreen to participants)

WELCOME TO THIS ACADEMIC STUDY ABOUT FINANCIAL SERVICES EMPLOYEES AND PERSONAL TECHNOLOGIES

This research will examine how employees make use of personal smartphones, tablets and other technologies. The findings will be used to identify whether use of personal technologies should be a consideration when assessing cyber risk in the workplace. You have been invited to participate because you are employed by a financial organisation. If you choose to take part, your responses, thoughts and comments will be important to this study.

PLEASE TAKE THE TIME TO READ THE FOLLOWING PRIVACY NOTICE .

The electronic survey will not collect your IP address, email address nor request any personal data. Privacy of participants is protected by UK/EU industry standard encryption methods. The information that you provide will be held and processed in compliance with the Data Protection Act 2018, the General Data Protection Regulation (GDPR) and subsequent legislation. The survey provider is compliant with GDPR data collection requirements, uses UK/EU based servers and is certified to internationally recognised standards for information security management (ISMS).

The information collected by the survey will be used by Raichel Collis, r.collis@derby.ac.uk in the context of her PhD research with the University of

Derby. The aggregated findings will be presented in a PhD thesis which may later be academically or professionally published.

The lawful basis for collecting and processing this data is that it forms part of a degree programme of study at the University of Derby. All data connected with the project will be retained until project completion when the student has received their grade and degree award following submission of their work. It is anticipated that the data will be securely destroyed by 31 July 2020. As a data subject you can request withdrawal of consent by contacting the University Data Protection Officer James Eaglesfield on (01332) 591762, the Deputy DPO Helen Rishworth (01332) 591954 or by email to gdpr@derby.ac.uk

I give my explicit consent for my data to be used as stipulated.

○ YES ○ NO.

The survey takes approximately 12 minutes to complete. The following questions will include use of devices, technological ability, cyber awareness and, if relevant to you, the Internet of Things. Answers can be reviewed or amended while the survey is in progress. You may leave the survey at any time.

PERSONAL CODE FOR WITHDRAWAL PURPOSES. Please create a unique code in the field below, using 3 letters and 3 numbers. Do not use a date of birth or name. Keep your own copy of the code. To withdraw, email r.collis@derby.ac.uk and use the code as the subject heading with the word 'withdraw'. After 14 days, all survey data will be aggregated, and it will no longer be possible to identify your specific responses.

2. Self-Completion Questionnaire

FINANCIAL SERVICES EMPLOYEES AND PERSONAL TECHNOLOGIES

Section 1. Mobile devices

1. FILTER QUESTION. Do you work in any of the following financial services?

Please tick the appropriate box

I do not work in financial services

Bank

Building Society

Insurance

Mortgage

Any other financial services organisation not listed above (please specify):

2. FILTER QUESTION. Do you own any of these mobile devices for personal use?

If you own no mobile devices, please indicate.

I own no mobile devices

Smartphone

Tablet

iPad

Any other mobile device (please specify):

3. Please indicate all the activities you do with your device(s)

Read and write emails.

Use messenger / chat / communication apps e.g. WhatsApp, Messenger, SnapChat.

Download free music.

Download videos.

Play games with other online gamers.

Shop from online retailers e.g. Amazon

Visit online casinos

Visit dating apps e.g.: OKCupid, Plenty of Fish, Tinder, etc

Download apps

Post on social media e.g. Facebook, Instagram , Twitter etc Shop from online auctions e.g. eBay.

Visit ‘adult’ websites.

Stream recently released films and new media.

Manage bank accounts

Any other activity not listed above

4. FILTER QUESTION.

If you indicated previously that you own more than one mobile device for personal use, which device would you most likely use to do the activities in the previous question? Please state the device in box A.

If you would use all your personal devices to do the activities from the previous question, please write YES in box B.

If you only have one personal mobile device, please write YES in box C.

A. I would use this device most... B. I would use all my devices....

C. I only have one personal mobile device.

5. Filter question. Do you take your device(s) with you to your workplace?

Yes

No

I don't take all my mobile devices to work

6. Does your device connect to the company network or company Wi-Fi when you are at your workplace?

Yes / Sometimes / No / Don't know

7. Where do you keep your device during work hours?

On my desk or workstation

In my bag at my desk or workstation

In my pocket

In a locker

Other (please specify):

8. Do you use your device(s) for work related activities? At home or out and about, e.g. on public transport or at a coffee shop with Wi-Fi connectivity.

No / Yes / Sometimes

If yes or sometimes, please say which work related activities.

9. Do you protect your device(s) with a password, code, pattern or other method e.g. image or voice-activation?

NO / YES

10. Do you use your device(s) for social networking? Yes /Sometimes /No

11. Do you do any of these activities while you are in your workplace?

(either on a break or during work hours)

ALWAYS / QUITE OFTEN / SOMETIMES / VERY / RARELY / NEVER

Download apps or software for personal use.

Download software updates from the internet, e.g. to update software you need for work. for example Adobe or Java.

SEND personal files FROM your mobile device to a colleague's device using bluetooth e.g. music or photos.

Post images, comments, or other content onto social media sites.

Play internet games. For example, on Facebook or other multi-user games.

ACCEPT personal files sent TO your device by Bluetooth e.g. media or photos.

Visit online casinos.

Send or receive work-related files or data by Bluetooth.

View media files, for example, films or videos streamed from file-sharing sites or crypto lockers.

12. Do you do the activities listed in the previous question, using your personal mobile device, or a company owned device? For example, a desktop computer or laptop. Please indicate all that apply.

My personal mobile device (smartphone, tablet, iPad etc)

A company desktop computer.

A company laptop.

A company issued tablet or iPad.

A company issued Smartphone.

13. How many apps have you downloaded to your device(s)? (Apps that you have searched for and downloaded yourself)

Less than 10

11 - 20

21 - 30

More than 30

Any comments?

14. FILTER QUESTION. Do you use Anti-Virus software on your personal mobile devices

Yes / No …….

14 a. I don't use anti-virus software because.....

15. If you receive an alert on your device(s) to update the operating system or an app or software, which response applies to you?

I don’t know how to update apps, software, or my operating system.

I ignore those messages as I have no time to update things.

I sometimes update my apps, software or operating system if prompted by the manufacturer.

I will always update my apps, software or operating system when prompted.

Section 2 Technological Ability

The following section will ask you about your knowledge of technology. You can change your answers at any time if necessary.

Please indicate your proficiency in the following areas.

None - no ability basic - working knowledge good - competent High - considerable knowledge Excellent - advanced knowledge

Operating computers such as a desk-top, or a laptop.

Operating mobile devices such as a tablet, iPad or a smartphone.

Locating software or an app on the internet and downloading it to a mobile device or a computer.

Using new apps and software for the first time.

Using system files on a computer or laptop.

Changing settings on a mobile device to suit your preference.

17. Are any of the following true about you? Please indicate whichever you feel is correct

TRUE / NOT TRUE

I don't know how to remove apps or software from my device or computer.

Technical vocabulary confuses me.

I don't understand technology and am not comfortable using it.

18. Do you do any of the following? Please indicate.

ALWAYS / QUITE OFTEN /SOMETIMES / VERY RARELY / NEVER

Customise web browsers with add-ons and plug-ins.

Delete cookies to prevent internet tracking

Sync browser data across all my devices

Use cloud sites to share and store files.

19. Please indicate if any of the following apply to you?

NOT TRUE /SOMETIMES TRUE /TRUE

I need guidance when doing something for the first time on a computer or mobile device.

I find new software or apps confusing

I make mistakes when using technology

21. Please assess your competency using the sliding scale:

0 = None

1 = Basic

2 = Good

3 = High

4 = Advanced

5 = Expert

Writing code. 0……5

Developing apps or software. 0……..5

Using blogging platforms like WordPress. 0…….5

Online multiplayer gaming. 0……..5

Using Virtual Reality. 0…….5

Any comments?

Section 3 Internet of Things and 'Smart' Technologies

The following questions will be about internet-connected devices. Please look at the examples listed below before answering the questions.

Voice Activated Personal Assistant : ALEXA, CORTANA, SIRI etc

Wi-Fi Music System: SONOS etc

Home heating or lighting system: NEST or HIVE etc

Home Surveillance system: INDOOR or OUTDOOR WEBCAMS, etc.

Home Security system: DOOR LOCKS, VIDEO DOORBELLS, etc.

Smart appliances : KETTLE, LAWNMOWER, FRIDGE, etc

22. FILTER QUESTION. Do you own any of the above, or any other internet-connected appliances or smart systems?

Yes / No / I don't know

23. Which of the following Internet of Things devices do you own?

Home Virtual Assistant

Wi-Fi Music system

Home Heating / lighting system

Home surveillance system

Home security system

Smart appliance

If your appliance or system is not listed above, please say what it is.

If you indicated that you own a smart appliance, for example, a hoover, fridge, or lawnmower, please would you say what your device is.

24. When you installed your smart device, did you change the default password to one of your own choice?

Please indicate the correct answer.

Yes / Maybe / I can't remember / No

Internet of Things: Wearable Devices

Please see the following list of wearable devices before answering the questions.

Fitness tracker: FITBIT, HUAWEI etc

'Smart' Watch : APPLE WATCH, SAMSUNG GALAXY WATCH etc

Health Monitor : GLUCOSE, INSULIN, BLOOD OR HEART RATE MONITORS.

'Smart' Clothes: INTERNET-CONNECTED T.SHIRT, JEANS or other garments.

'Smart' Footwear: TRAINERS etc

'Smart' Jewellery: NECKLACES, BRACELETS, RINGS etc.

25. FILTER QUESTION. Do you own a 'Wearable' device like any of the ones listed above?

If you do not own a wearable device but indicated in the previous question that you own a smart system or appliance, please tick the appropriate box.

YES. I do own a wearable device.

NO. I do not own a wearable device.

I DO NOT own a wearable device, but I DO own a smart system or appliance.

I don't know.

26. Which of the following 'wearable' Internet of Things devices do you own?

Fitness Tracker

Smart Watch

Health monitor

Smart clothing

Smart footwear

Smart jewellery

If you own a wearable device not on the list, please would you say what it is.

27. Do you wear your device in the workplace?

Always / Sometimes / Never

28. Does your device connect to the company network?

Yes / Sometimes / No / Don’t know

29. FILTER QUESTION Does your device use an app for control or access?

Yes / No

30. FILTER QUESTION Is the app downloaded onto your mobile device(s)?

Yes / No

Please say which to which device (s)

31. FILTER QUESTION. Do you have any apps downloaded to your mobile devices which control Internet of Things devices you do not own personally?

For example, door entry systems or environmental controls in the building where you live, or other Internet of Things devices you use that are owned by others.

Yes / No

32. Please say what other Internet of Things devices you have apps for?

33. Please state the total number of Internet of Things control apps downloaded onto your mobile devices(s)

This includes apps for any devices you own and any others you might use.

34. FILTER QUESTION Do you access your smart devices while you are at your workplace? No / Sometimes / Yes

35. Do you access your smart devices during break times or during working hours?

Break time

Working hours

Both breaks and working hours

36. When you access your Internet of Things device(s) at work, do you use the app on your mobile device or visit your account on the desktop website?

App / Desktop Website / Both

37. Why do you access your Internet of Things device(s) while you are at work?

Please explain.....

38. Do you update your Internet of Things device(s) when advised by the manufacturer?

Yes / Sometimes / No

39. FILTER QUESTION Did you research the Internet of Things device(s) before your purchase, to make sure of built in security controls?

Yes / No / Comments:……..

40. I did no research about security before buying my device(s) because.....

I wanted this type of device and bought one that suited my lifestyle

My device was a gift

My device was an impulse purchase without any planning Any other reason?

Section 4. Cyber Awareness

We are interested to know how you use the internet. Please remember you are anonymous and can change any of your answers at any time.

41. FILTER QUESTION Do you have a profile on any of the following social networks?

Please indicate all your profiles, or if you have no profiles, please tick the appropriate button.

None of these

Facebook

Twitter

Instagram

42. How often do you post any of the following content?

ALWAYS /OFTEN /SOMETIMES / VERY RARELY / NEVER

Photographs of me (selfies).

Photos of my partner or spouse.

Photos of my children.

Photos of my family (parents, siblings etc).

Comments about my spouse or partner.

Comments about my family (parents, siblings, etc).

Comments about my children.

Comments about my hobbies, interests and social activities.

Comments about my friends.

43. How likely are you to do any of the following whilst social networking?

NEVER /VERY RARELY /SOMETIMES/ QUITE OFTEN /ALWAYS

Open a link which promises you a free gift card or prize.

Accept a friend or follower request if you don’t know or recognise the person.

Follow a link that claims to reveal who has been viewing your profile page.

Provide a personal email address to win a free gift or prize.

Click on a link shared by a friend, to see some sensational or trending content.

Click on a link shared by someone you don't know, because the content looks appealing.

Respond to an unsolicited private message from someone not part of your social network.

44. FILTER QUESTION. Do you have a LinkedIn profile?

Yes / No

45. Does your LinkedIn profile contain any of the following information?

Please tick all that apply.

The name and location of the primary school you attended.

The name and location of the school you attended for secondary education.

Any voluntary work you currently do or have done in the past.

The names of clubs or societies you attend in your free time.

Any fundraising you have taken part in, either alone or as a group.

Your hobbies or interests outside work.

Any sports you take part in, or a sports team you are a member of.

46. FILTER QUESTION Do you use any of the following messaging apps or services? (If you do not use messaging apps or services, please tick the NO button)

No. I do not use any Messaging Apps or services

WhatsApp

Facebook Messenger

Snapchat Telegram

Blackberry Messenger

Yahoo Messenger

Any other messaging services

47. Do you respond to new messages or comments during work time?

- No

- Sometimes
- Yes

48. If you received any of the following emails, would you open them?

DEFINITELY NOT /PROBABLY NOT/ POSSIBLY/ PROBABLY/ DEFINITELY

An email from the National Lottery saying you have won some money.

An email from HMRC saying you are due a tax rebate.

An email from your bank saying your account has been compromised.

An email from the police saying you have been caught on a speed camera.

An email from a company you don't recognise saying that your invoice is attached.

An email from a friend or colleague but with poor spelling, grammar or strange words.

49. When you download an app, do you pay for it or choose a free one?

- Pay
- Free
- Both

50. How likely are you to do the following?

ALWAYS /QUITE OFTEN/ SOMETIMES /VERY RARELY/NEVER

Accept your work colleagues as friends or followers on social media.

Use the same passwords for all online accounts.

Enable privacy controls on social media profiles to protect privacy.

Only enable bluetooth on your devices when sending or receiving files

Check to make sure you are visiting genuine websites when browsing the internet.

Use the 'log out' button to log out properly when leaving any financial or payment website e.g., a bank, or PayPal.

Check for the padlock symbol before entering financial details to make an online payment

Use NFC on your smartphone to make payments or share content

Delete any apps or programs no longer used.

Use passwords compiled from personal details e.g. the name of a child or pet, date of birth etc

DEMOGRAPHIC QUESTIONS

51. About You.....

- Male
- Female
- Other
- Prefer not to say

52. Your Age?

- 18-24 25-34 35-44 45 – 54 55 - 65
- 66 plus Prefer not to say

53. Nationality? …….

54. What is your highest level of education?

- School
- College
- Vocational
- Professional or Industry
- University
- Prefer not to say
- Other (please specify):

55. Your Employment? Your position in the company is?

- Executive
- Senior Manager
- Middle Manager
- Manager/supervisor
- Clerk /Officer/Associate/ Admin /Front line staff
- Prefer not to say
- Other (please specify):

57. Employment Status?

Full-time employee /Part-time employee /Prefer not to say

3. Debrief Document **(As seen on screen at the end of the survey**

THANK YOU FOR TAKING PART IN THIS RESEARCH STUDY

The purpose of this study is to investigate whether the use of personal technologies should be a consideration when assessing cyber risk in the workplace. The financial sector was chosen as a research subject due to the high volume of technological systems in use and the potential for cyber security breaches.

RIGHT TO WITHDRAW. Requests to withdraw should be emailed to **r.collis@derby.ac.uk** using your personal code as the subject heading and include the word 'withdraw'. The withdrawal period is available for 14 days after submitting the survey, after which time the data will be aggregated and it will no longer be possible to remove specific data.

DATA PROTECTION. The information that you supply for this online survey will be held and processed in compliance with the Data Protection Act 2018, the General Data Protection Regulation (GDPR) and subsequent legislation. If you have any concerns about Data Protection, please contact James Eaglesfield, Data Protection Officer, University of Derby (01332) 591762 or the Deputy DPO Helen Rishworth (01332) 591954. Alternatively email **gdpr@derby.ac.uk**. Further information about Data Protection / GDPR can be found at the Information Commissioner's website. Available at: **www.ico.org.uk**

APPROVAL. This research study was approved by the College Research Ethics Committee at University of Derby. If you have any comments or questions or

would like to view the findings of the research after assessment of the written paper, please email the researcher. If you have any concerns regarding the project, please contact the project supervisor Dr David Hicks, PhD at **d.hicks@derby.ac.uk** 01332 592871**.**

RESOURCES.

If you have experienced cyber-crime, including scams, fraud and phishing attempts, you can report it using Action Fraud, the national fraud and cyber-crime reporting centre. Available at: **www.actionfraud.police.uk.** For information about protecting yourself online, these websites offer valuable resources:

www.staysafeonline.org A global initiative to educate about online safety.

www.getsafeonline.org A UK source of information regarding online safety.