# UNIVERSITY OF SOUTHAMPTON

FACULTY OF SOCIAL, HUMAN AND MATHEMATICAL SCIENCES

Social Sciences

**Responsibilisation, Rules and Rule-following concerning Cyber Security: Findings from Small Business Case Studies in the UK.**

by

**Neil MacEwan**

Thesis for the degree of iPhD Web Science (Soc Sci)

September 2017

**UNIVERSITY OF SOUTHAMPTON**

# ABSTRACT

**FACULTY OF SOCIAL, HUMAN AND MATHEMATICAL SCIENCES**

Thesis for the degree of iPhD Web Science (Soc Sci)

**Responsibilisation, Rules and Rule-following concerning Cyber Security: Findings from Small Business Case Studies in the UK.**

Neil MacEwan

This thesis is the result of an investigation into the challenges that lie within the governance of small business employees' behaviour towards cyber security. That investigation comprised three stages. The first was an exploration of the political context in which the matter of cyber security sits within the UK. This sought to determine whether cyber security is a policy area where the State continues to push responsibility away from itself and onto non-State actors, as a means of extending and enhancing the governance of situations and environments which have a tendency to produce criminal behaviour (Garland, 1997). More specifically, the research questions explored during this stage were: **In the UK, is government discourse responsibilising small businesses, and the people who work within them, for cyber security? If so, how? And with what implications?** Answering these questions involved detailed analysis of much government discourse on cybercrime and cyber security. It was found that the UK government continues to employ a responsibilisation strategy in the governance of cybercrime and cyber security. Yet, it has become increasingly frustrated with what it sees as poor risk management by those so responsibilised, such as small businesses. This has caused the government to speak in more judgemental and less tolerant terms on this matter, and thereby also continue to shape victim status in ways that make it increasingly difficult to attain. In turn, this brings consequences which include the danger of victim blaming.

The second and third stages of research sought to evaluate that continuing governmental strategy of responsibilisation 'on the ground.' In particular, to learn how small businesses are coping with the 'responsibilisation conundrum' passed on to them by the government: that of getting *each* of their employees to behave in cyber-

secure ways, *all* of the time. The specific research questions explored during these stages were: **Within their everyday working lives, do employees within small businesses practise what their government and their employers preach to them about cyber security? And if not, why not?** Answering these questions involved the conduct of case studies within three small businesses. These comprised a five-day Diary Study, followed up by semi-structured Interviewing. Collectively, the findings from these case studies indicated strongly that the government has underestimated the difficulty of that 'responsibilisation conundrum.' Specifically, by showing that the governance of employees' behaviour around cyber security within small businesses, in and beyond the workplace, can be far from straightforward, in a number of ways and for a number of reasons.

However, this research has also gone on to demonstrate that this 'responsibilisation conundrum' is *even more difficult* than has been recognised before, by the government or anyone else. Specifically, because the matter of rules and rule-following behaviour brings greater complexity to it. Two aspects of this research have combined to shed new light on that 'responsibilisation conundrum': Firstly, further findings from those case studies have provided much evidence of the *real* influences on people's rule-following behaviour around cyber security, the most potent of which were found to be pragmatism ('just getting things done') and consensus ('that's how we all do it here'). And secondly, the first application of Meaning Finitism and Rule Scepticism within the subject of cyber security has challenged strongly some assumptions being made by government and businesses about the efficacy of rules and their use in the governance of cyber security.

All of these findings have led to two main recommendations: Firstly, that in future any strategies for governing the human aspects of cyber security should be *grounded* in people's lived experiences of cyber security within their everyday working lives. And secondly, as part of a solution to the 'responsibilisation conundrum,' a Finitist approach should now be taken to training and otherwise guiding people towards cyber-secure behaviours. Combining a true understanding of the relation between rules and conduct, and a recognition of the multiplicity of cyber security threats, this is an approach that will help shape the behaviour of employees in ways sought but seldom achieved by rule-setting.

# Table of Contents

**Abstract** ..... i

**Table of Contents** ..... iii

**List of Accompanying Materials** ..... vii

**Declaration of Authorship** ..... viii

**Acknowledgements** ..... ix

**Abbreviations** ..... x

**Chapter 1: Introduction** ..... 1

1.1 Research Objectives ..... 2

1.2 Disciplines, knowledge and methods drawn upon ..... 2

1.3 The key arguments that will be made ..... 3

1.4 Chapter Summary ..... 4

**Chapter 2: Literature Review** ..... **6**

2.1 Introduction ..... 6

2.2 Responsibilisation ..... 6

2.2.1 Victim Blaming ..... 11

2.3 Positivist Victimology ..... 12

2.4 Critical Victimology ..... 16

2.5 Further ambient pressures ..... 19

2.6 The use of training and rules in the governance of behaviour ..... 21

2.6.1 Shaping people's behaviour through training ..... 22

2.6.2 Governing people's behaviour through policy rules ..... 25

2.7 Rules, and rule-following behaviour ..... 26

2.7.1 Meaning Finitism ..... 27

2.7.2 Rule Scepticism ..... 29

2.7.3 Finitism and training ..... 30

2.8 Conclusion ..... 33

**Chapter 3: Research Methods** ..... **34**

3.1 Introduction ..... 34

3.2 Recruitment ..... 34
3.3 Documentary Analysis ..... 37
3.3.1 Framework Analysis ..... 38
3.4 Observation ..... 39
3.5 Diary Study ..... 39
3.6 Interviewing ..... 44
3.7 Transcription of the data from the DS and Interviewing stages ..... 47
3.8 Analysis of the data from the DS and Interviewing stages ..... 47
**Chapter 4: Documentary Analysis ..... 48**
4.1 Introduction ..... 48
4.2 Corporate and individual responsibility for cyber security ..... 50
4.2.1 The responsibilisation of organisations ..... 50
4.2.2 Heightening the rhetoric of responsibilisation ..... 54
4.2.3 The responsibilisation of individuals ..... 59
4.3 Victim Status ..... 63
4.3.1 Victim Precipitation ..... 63
4.3.2 Victim Blaming ..... 66
4.4 Conclusion ..... 70
**Chapter 5: Case Studies ..... 73**
5.1 Introduction ..... 73
5.2 The government's own attempts at guidance ..... 74
5.3 Employees want guidance on cyber security ..... 75
5.4 Problems with training ..... 76
5.4.1 Financial pressure ..... 77
5.4.2 Pitching to training needs ..... 80
5.4.3 'Training fatigue' ..... 81
5.4.4 Training preferences ..... 83
5.5 Problems with policy ..... 86
5.5.1 The existence of formal policy on cyber security ..... 86
5.5.2 Differing awareness and knowledge of policy ..... 88

5.5.3 Disengagement from policy ..... 91
5.6 Conclusion ..... 95
**Chapter 6: Rule-following ..... 98**
6.1 Introduction ..... 98
6.2 The existing rule sets ..... 99
6.3 Rules, and why we have them ..... 100
6.3.1 Questioning those three assumptions ..... 102
6.4 Predispositions/conventions within rule-following behaviour .. 106
6.4.1 Personal traits and tendencies ..... 107
6.4.2 Personal interest, or lack of interest ..... 108
6.4.3 Personal perspectives on technology and cyber security ..... 109
6.4.4 Professional experience and job status/level ..... 112
6.4.5 Workload and worktime pressure ..... 114
6.4.6 Technological obstacles and 'workarounds' ..... 117
6.4.7 Anticipation of formal sanctions ..... 120
6.4.8 Being busy, serving immediate purposes and pragmatism ..... 124
6.4.9 Interaction with others, and 'just what people here do' ..... 130
6.5 Conclusion ..... 134
**Chapter 7: Discussion ..... 136**
7.1 Introduction ..... 136
7.2 The complexities of responsibilisation ..... 136
7.2.1 Why government advice and business strategy must change 138
7.2.2 The complexities of shaping/controlling employee behaviour 138
7.2.3 Can any of these findings be generalised? ..... 141
7.3 Given these new findings, what should be done? ..... 142
7.3.1 A new way of responsibilising small business employees ..... 142
7.3.2 A two-stage solution to the 'responsibilisation conundrum' .. 143
7.4 Conclusion ..... 146
**Chapter 8: Conclusion ..... 147**
8.1 Key findings and Conclusions ..... 147

8.2 Policy recommendations ..... 150

8.3 Encouraging signs of change in the government's perspective . 151

8.4 Future work..... 151

**List of Appendices ..... 154**

Appendix A..... 155

Appendix B..... 166

Appendix C..... 171

Appendix D..... 175

Appendix E ..... 178

Appendix F ..... 179

Appendix G ..... 183

Appendix H..... 208

Appendix I ..... 209

Appendix J..... 241

Appendix K..... 242

Appendix L ..... 244

Appendix M..... 245

**Bibliography ..... 250**

Word Count (excluding Appendices and Bibliography): 59,771

# List of Accompanying Materials

**Appendix A:** **Redacted copies of the relevant sections of Business B's Office Manual** – page 152.

**Appendix B:** **Business C's Social Media Policy (extracted from its Staff Handbook)** – page 163.

**Appendix C:** **Business C's ICT Induction Document** – page 168.

**Appendix D:** **'Notes on how to use Business C's IT system' Document** – page 172.

**Appendix E:** **Listing of the thematic framework used in the Documentary Analysis** – page 175.

**Appendix F:** **List of the twenty-five documents analysed during the Documentary Analysis** – page 176.

**Appendix G:** **The data from the Documentary Analysis set with the thematic framework** – page 180.

**Appendix H:** **Listing of the thematic framework used in the analysis of the data collected during the Case Studies** – page 205.

**Appendix I:** **The data from both stages of the Case Studies (Diary Study and Interviewing) set within the thematic framework** – page 206.

**Appendix J:** **Recruitment Advert** – page 238.

**Appendix K:** **Participant Information Sheet** – page 239.

**Appendix L:** **Consent Form** – page 241.

**Appendix M:** **Diary Study Questions** – page 242.

# Declaration of Authorship

**I, Neil MacEwan, declare that this thesis and the work presented in it are my own and have been generated by me as the result of my own original research.**

**Responsibilisation, Rules and Rule-following concerning Cyber Security within Small Businesses in the UK.**

**In confirm that:**

1. **This work was done wholly or mainly while in candidature for a research degree at this University;**
2. **Where any part of this thesis has previously been submitted for a degree or any other qualification at this University or other institution, this has been clearly stated;**
3. **Where I have consulted the published work of others, this is always clearly attributed;**
4. **Where I have quoted from the work of others, the source is always given. With the exceptions of such quotations, this thesis is entirely my own work;**
5. **I have acknowledged all main sources of help;**
6. **Where the thesis is based on work done by myself jointly with others, I have made clear exactly what was done by others and what I have contributed myself;**
7. **None of this work has been published before submission.**

**Signed:** *Neil MacEwan*

**Date: 14th September 2017.**

# Acknowledgements

Firstly, I would like to thank my supervisory team for all their help, advice and support. They are: Dr. Gethin Rees (University of Newcastle), Dr. Kieron O'Hara (University of Southampton) and Dr. Craig Webber (University of Southampton). I would also like to thank Dr. Tim Chown, who was on the supervisory team for the first two years (before leaving the University of Southampton).

And secondly, I would like to thank all of the research participants, each of whom completed all components of the case studies.

# Abbreviations

| | |
|---|---|
| **DBIS** | **Department for Business, Innovations and Skills** |
| **DCMS** | **Department for Culture, Media and Sport** |
| **FSB** | **Federation of Small Businesses** |
| **GCHQ** | **Government Communications Headquarters** |
| **GDPR** | **General Data Protection Regulation** |
| **ICO** | **Information Commissioner's Office** |
| **IoD** | **Institute of Directors** |
| **ISO** | **International Organization for Standardization** |
| **LRAT** | **Lifestyle/Routine Activity Theory** |
| **NISD** | **Network and Information Security Directive** |

# Chapter 1: Introduction

In late modernity[1], fear and uncertainty have accompanied the acceleration of technological change and globalisation. We live in a 'risk society,' preoccupied with safety and in relentless pursuit of security (Beck, 1992; Giddens, 1990). Amid this existential anxiety, the rise of Neoliberal politics has brought a 'culture of control' (Garland, 2001) within which citizens and organisations have been required to manage their own crime risks (O'Malley, 1992). Such responsibilisation is a key feature of the Neoliberal approach to governance, through which the downsized State governs from a distance (Garland, 2001; Loader and Sparks, 2002; Brown, 2006;).

At first glance, the field of cyber security seems well-suited to this regulatory model because, by its very nature, cyberspace challenges the ability of governments to regulate human behaviour and protect citizens and businesses (Lessig, 2006; Reed, 2012). It epitomises the distanciation of time and space within late modernity (Giddens, 1990), and cybercrime is a form of disorder that comes from it. Cyberspace changes crime victimisation. Offline, the limitations of time and travel reduce the range and number of potential victims. Online, however, presence and absence have been connected (Giddens, 1990). In cyberspace – described by some as 'anti-spatial' (Mitchell, 1995) – one person may offend against many, concurrently and from any distance.

Online also, victimhood often *feeds* further criminality. This means that cybercrime victimisation can be initial, onward and ongoing. A ransomware attack exemplifies this. For example, an individual is targeted via a phishing email[2]. Unwittingly, they fall victim to it, and thereby enable the victimisation of the business for which they work. With crucial files now encrypted (and not backed up), that business experiences increasing pressure to pay the ransom. If it then fails to pay – or pays, but the

[1] Defined as 'the distinctive pattern of social, economic and cultural relations that emerged in America, Britain and elsewhere in the developed world in the last third of the twentieth century' (Garland, 2001, p.viii).

[2] 'Phishing' is a form of fraud using tactics of social engineering, in which the attacker tries to trick people into revealing personal information (e.g. login credentials or bank account passwords) by masquerading as a reputable entity or person within email, Instant Messaging or other communication channels. Typically, victims are engaged through email containing links to spoof websites.

promised decryption is not delivered – this can render other people/businesses victims of that same crime[3], or victims of further crimes that follow from it[4].

Crucially, another consequence flows from these changes in the nature of victimhood. It is that citizens, businesses and business employees are now viewed as potential victims *and* (unwitting) parties to cybercrime. This has a profound impact on the responsibilisation agenda. Today, people and businesses are expected to protect themselves *and others* from cybercrime. In this way, the prevention of cybercrime has become a heightened, or skewed, form of the 'co-production of order and security' (Loader and Sparks, 2002, p.89) within late modernity.

### 1.1 Research Objectives

In the research that has led to this thesis, I had three main objectives:

Firstly, I was keen to explore the political context in which the matter of cyber security sits. Specifically, I wanted to determine whether cyber security is a policy area where the State continues to push responsibility away from itself and onto non-State actors, as a means of extending and enhancing the governance of situations and environments which have a tendency to produce criminal behaviour (Garland, 1997).

Secondly, if such a responsibilisation strategy was found to exist, I wanted to determine whether government discourse is continuing to responsibilise *small businesses* for their own (and others) cyber security, and with what implications.

And thirdly, if such responsibilisation through government discourse was found to be continuing, I wanted to determine whether, within their everyday working lives, small business employees are *actually practising* what the government and their employers are preaching to them about cyber security; and if not, why not?

### 1.2 Disciplines, knowledge and methods drawn upon for this research

Within the disciplines of Cyber Security and Information Security, this research has drawn upon existing knowledge about the human aspects of cyber security,

[3] E.g. Data loss bringing personal, legal or commercial consequences.
[4] E.g. Identity Theft and/or further phishing attempts, leading to fraud. Indeed, according to research conducted by the anti-fraud organisation Cifas, Identity Theft is reaching 'epidemic levels,' with identities being stolen at a rate of almost 500 a day in the UK during the first six months of 2017 (Peachey and Johnston, 2017).

particularly the line of research that has challenged the notion that humans are the weakest link within, and thereby an enemy of, cyber/information security (Adams and Sasse, 1999, onwards). It has also reached into, and drawn knowledge from, other disciplines: From Political Science, about 'governance' and 'governmentality' (e.g. Foucault, 1978). From Sociology, about certain aspects of the Neoliberal approach to the governance of crime (e.g. Garland, 1997). From Victimology, about certain dangers (e.g. victim blaming) which can accompany that particular approach (e.g. Walklate, 1997). From Philosophy, about the use of language within rules and rule-following behaviour (e.g. Wittgenstein, 1967), and from Sociology, certain theories and approaches (Meaning Finitism and Rule Scepticism) linked strongly to those philosophical reflections (e.g. Barnes *et al*., 1996; Bloor, 1997).

Drawing upon this collective knowledge has helped in the achievement of the aforementioned research objectives; specifically, by shedding light on the political context within which cyber security sits, the realities of the use language in the shaping of behaviour, and the true influences upon rule-following within everyday working life.

The choice of methods made for this research was influenced partly by certain work done previously in the field of Information Security; specifically, research involving the use of Diary Study (Steves *et al*., 2014), and the use of semi-structured interviewing following Diary Study (Inglesant and Sasse, 2010).

### 1.3 The key arguments that will be made

This thesis will argue that, in the UK, the State has very much underestimated the difficulties that small businesses face in the design and successful implementation of strategies which seek to get *each* of their employees to behave in cyber-secure ways, *all* of the time – what I have termed the 'responsibilisation condundrum.'

It will then go on to argue that such underestimation of the complexity of this conundrum – by both the government and small businesses themselves – comes from their naïve and mistaken understanding of the use and efficacy of rules, and of rule-following behaviour.

Then, it will present a more accurate analysis of rule-following *in practice*, drawn from two connected schools of thought: Meaning Finitism and Rule Scepticism. These

approaches will be applied 'on the ground' during case studies in three small businesses, revealing the *true* influences upon people's rule-following behaviour.

Lastly, specific recommendations will be made for policy changes within strategies which seek to govern the human aspects of cyber security within small businesses.

### 1.4 Chapter Summary

In this first chapter, I have explained my research objectives and given in summary what this thesis will go on to argue. In Chapter 2 (Literature Review), I will discuss why I have done my research, and how it relates to other research in the fields of study with which it connects. By doing so, I will justify and situate the research questions that have framed and driven my research project. In Chapter 3 (Research Methods), I will discuss how I researched those questions. Mainly, this will involve outlining my chosen research methods and commenting on their use, but will also include some initial discussion of how I recruited the research participants.

In Chapter 4 (Documentary Analysis), I will report and comment upon the themes and subthemes that I identified during my analysis of many documents concerned with government and commercial discourse on cyber security and cybercrime victimisation. Through this, I will highlight the ways in which responsibility is being placed upon small businesses for their own cyber security, and that of others with whom they trade and communicate. Although the majority of this chapter will be focused on political rhetoric and discourse, it will also include discussion of some non-government and near-government organisations that are involved in reproducing and reinforcing those governmental narratives, such as banks and the police.

In Chapter 5 (Case Studies), I will investigate whether *in practice* – through training and policy – small businesses have been trying to govern their employees' behaviour in the way that the State has told them to; and if so, how difficult and how effective that has been. This will involve presenting results from my case studies. These will demonstrate that, in a number of ways and for a number of reasons, such responsibilisation of employees is *more complicated* than the government perceives it to be; and that, consequently, it has underestimated this pivotal task.

In Chapter 6 (Rule-following), I will argue that this 'responsibilisation conundrum' is *yet more difficult* than anyone (including the government) has realised. I will

demonstrate this, first by introducing a much more accurate understanding of rules and rule-following that is supplied by Meaning Finitism and Rule Scepticism, and then by presenting further findings from my case studies which provide much evidence of the *true* influences upon people's rule following behaviour.

In Chapter 7 (Discussion), I will discuss the full evidential picture that has emerged from my research. That picture provides a more enlightened view of the evermore important task of governing people's behaviour around cyber security. My discussion of it will include calls for change in the government's thinking, and its advice to the business sector. It will also set out ways to solve the problems of responsibilising employees for cyber security within small businesses.

In the final Chapter (Conclusion), I will reiterate my key findings and conclusions, and summarise again my policy recommendations. Lastly, I will discuss plans for future work.

# Chapter 2: Literature Review

## 2.1 Introduction

Increasingly, we 'live' in cyberspace. Our inhabitance of it, and reliance upon it, is plain to see. Daily lives, fundamental rights, social interactions and economies depend on its inherent technologies 'working seamlessly' (European Commission, 2013, p.2). Governments have come to view it also as an environment in and through which national security can be threatened. Since October 2010, the UK government has equated the threat of cybercrime with international terrorism and military crises, within what it has termed 'an Age of Uncertainty' (HM Government, 2010, pp.3 and 27). Consequently, it has continued to place responsibility on the public to look after their own cyber security. Indeed, it feels as if there has been a striking increase in the strength and prevalence of that responsibilisation message. In particular, the government has been urging businesses within the SME sector to improve their cyber security. Crucially, this involves them getting *all* of their employees to accept, and then *practise*, individual responsibility for cyber security. In essence, my research has been investigating the safety and efficacy of this strategy. More specifically, it has been exploring the difficulties that lie within this approach, providing more accurate explanation of why those difficulties occur, and identifying measures which could be used to address some of them.

In this chapter, I will discuss why I have done my research and how it relates to other research in the fields of study with which it connects. In this way, through this literature review I will justify and situate the research questions that have framed and driven my research project.

## 2.2 Responsibilisation

It is important to set my research within the wider context of the consequences of late modernity. The confluence of Neoliberal politics with the risks and insecurities of late modernity shaped the response to crime within a new 'culture of control' (Garland, 2001), which then remodelled crime control on a more dispersed, partnership basis: the State would now work *through* civil society, and not *upon* it. Key to this strategy of governing from a distance was getting non-State actors, including individual citizens, to take responsibility for preventative action against crime. Among other

things, my research has sought to determine whether that strategic, governmental approach is being taken on the subject of cyber security.

Given also that my research has a strong criminological element to it, it is important to show as well the rise of Neoliberal influence within Criminology itself. In the UK, the origins of citizen responsibilisation in the prevention and control of crime can be traced back some fifty years. Since then, in many ways, the only societal constant has been change. Collectively, some particular movements, advances and alterations have formed the ground from which that responsibilisation has grown (Garland, 2001): government from increasing distance, insecurity from rising crime, strategic shift towards crime prevention, and increasing concern with crime victimisation. Charting an historical course through this sea of change will provide more contextual understanding of the government discourse around citizen responsibilisation for cyber security.

In 1960s-70s Britain, high crime emerged from profound social and spatial change. The social fabric had been stretched, time and space distanciated, and civil society thereby rendered more porous and vulnerable (Giddens, 1990; Garland, 2001). Previously, crime and incivility had mostly affected the poor. Now, the social distance between the middle classes and crime was greatly reduced, bringing with it 'consequences for point of view and perspective' (Garland, 2001, p.152). Seeds of insecurity grew. Unintentionally, the State's strategic response to rising crime only increased public anxiety. Its focus on serious crimes, and toleration of lesser crimes, led many to believe that it was beating a retreat. This gave people a disturbing sense of a 'control deficit' (Garland, 2001), which formed part of a broader crisis of public confidence in the 'rehabilitative ideal' and the efficacy of the Criminal Justice System (Crawford and Evans, 2012). Penal welfarism had fallen into disrepute. In rehabilitative treatment, it was claimed, nothing worked (Martinson, 1974), and there were strong calls for a criminological focus on achievable public policy goals (Wilson, 1975). Facing this predicament, the State would soon withdraw its claim to be the chief provider of security. This formed part of a wider shift from government to governance. Seen through the Foucauldian lens of 'governmentality,' it was a movement towards the deployment of various techniques, strategies and rationalities for managing economic, social and individual activity (Foucault, 1978; Rose and Miller, 1992; Garland, 1997). Viewed in terms of a 'differentiated polity' (Rhodes, 1997),

government institutions would now concentrate on 'steering' rather than 'rowing' (Osborne and Gaebler, 1992). From either perspective, change came through the fragmentation and diffusion of power (Loader and Sparks, 2002).

Previously, through deference to 'expert' judgement, crime control had been shielded from political scrutiny (Crawford and Evans, 2012). Now, however, it drew criticism from both ends of the political spectrum. Penal welfarism was attacked by Liberals for its unfairness, and by Conservatives for its inefficiency, as law and order became the subject of keen political debate. High crime and insecurity were being seen as normal facts of late modern life, two of the risks flowing from the threatening force of modernisation and its globalisation of doubt (Beck, 1992; Giddens; 1990). Yet, the perception of risk is culturally constructed (Beck, 1992; Wildavsky, 1988), and its presentiment inherently political (Loader and Sparks, 2002), and by the end of the 1970s the changes brought by late modernity had given rise to a new politics. Incoming Neoliberal governments in Britain (1979) and America (1981) supported a focal shift from the causes to the consequences of crime, and embraced the concept of crime prevention. It chimed with key aspects of their political rationality: rolling back the State, viewing citizens as rational economic actors, and pursuing the business principle of loss minimisation. Although that political rationality was clearly based on a certain conception of the market, these ideas on the governance of people and crime were not simply leakage from the economic to other spheres; they were 'the explicit imposition of a particular form of market rationality on those spheres' (Brown, 2006, p.693).

Within the aforementioned resulting 'culture of control' (Garland, 2001), 'privatised prudentialism' (O'Malley, 1992) would feature greatly in this co-production of security. Criminologists looked for approaches that would have some immediate policy and practical relevance (Newburn, 2013). What soon emerged were the 'criminologies of everyday life,'[5] which viewed crime as normal and continuous, 'a routine risk to be calculated or an accident to be avoided, rather than a moral aberration that needs to be specially explained' (Garland, 2001, p.128). The path of knowledge had turned away from the offender toward the victim and the offence. In particular, Lifestyle/Routine Activity Theory (LRAT) treated as important the

[5] Rational Choice Theory, Routine Activity Theory and Situational Crime Prevention.

distinction between criminality and crime, arguing that the motivation to offend was not the only prerequisite for the occurrence of a criminal event. The claimed 'chemistry of crime' (Felson, 1998) was the mixture of a motivated offender, a suitable target and the absence of capable guardians (Cohen and Felson, 1979). It was argued that the convergence of these three elements, in time and space, was a minimal requirement for every crime, and that the likelihood of such convergence was determined by the prevailing social conditions, the most influential of which was people's routine activities. This then led to claims that the routines of everyday life affect profoundly the opportunities for crime, and that people can influence their chances of falling victim to crime by reducing their targetability[6] (Cohen and Felson, 1979).

Throughout the 1980s in Britain, crime continued to rise. However, responsibilisation is integral to Neoliberal ideology (Hall, 2004; Brown, 2006; Rees and White, 2012), and its place within British crime policy seemed secure. In 1990, Prime Minister Thatcher remarked: 'We have to be careful that we ourselves don't make it easy for the criminal' (*The Age*, 28 September 1990). These words also served as a reminder that every system of risk management creates a blaming system as its counterpart (Sparks, 2001; Loader and Sparks, 2002). In this way, during the 1980s and 1990s crime victimisation and crime prevention became interwoven, with the targeting of 'irrationality' as a key thread. Initially, the policy view was that much of the fear of crime was irrational, and stemmed from ignorance (Gottfredson, 1984). Accordingly, people would be educated into taking informed decisions around 'real' risks (O'Malley, 2006). The government was requiring citizens to be active risk managers (Giddens, 1991; Beck, 1992), making prudent choices over lifestyle (Kemshall 2006; Castel, 1991). This was part of the ongoing reconfiguration of the relationship between the citizen and the State (Clarke and Newman, 1997; Manning and Shaw, 2000). Latterly, the thinking and the rhetoric around responsibilisation became more judgemental. Victims, potential and actual, would be expected to behave in ways which attracted least risk (Elias, 1993; Walklate, 1997). Crime risk 'became an individual issue, rather than a collective concern to be governed by individual choice' (O'Malley, 2006, p.52).

[6] Sometimes referred to as 'target hardening.'

In the mid-1990s, crime peaked shortly before the Conservative government was voted out of office. The incoming *New Labour* administration brought with it a commitment to crime prevention, influenced heavily by Communitarian philosophy (Etzioni, 1993). Initially, it seemed that this new perspective 'might offer a more progressive than punitive approach' (Crawford and Evans, 2012, p.798). However, while it distinguished *New Labour* from the hyper-individualised, Neoliberal crime policy of the previous government, Communitarianism had its own form of responsibilisation. It placed strong and recurrent emphasis 'on duties and responsibilities to the wider society rather than freedoms and rights for the individual' (Hughes, 2007, p.20). As the messages took on a 'moralistic and rightist' tone (Ibid, p.15), it became clear that, within what *New Labour* dubbed the 'something for something society' (Home Office, 2003, p.3), rights would be conditional on the exercise of responsibility (Crawford and Evans, 2012). Within Criminology, Left Realism had emerged in opposition to Right Realism[7], criticising it for, *inter alia*, ignoring the importance of socio-economic context in explaining crime, and for not exploring the relationship between offenders, victims and formal/informal controls, in what was termed 'the square of crime' (Young, 1992). However, while Left Realist thought could be detected in some of the rhetoric of the first *New Labour* administration (e.g. its emphasis on social inclusion), 'Labour governments shifted progressively from a position that was reasonably sympathetic to Left Realist thinking to one that was much more comfortable with Right Realist theory' (Newburn, 2013, p.275).

*New Labour* governed from 1997 until 2010. During that thirteen year period, crime prevention practice had once again been 'thrown up in the air…to find a new balance and focus under a myriad of 'owners'' (Crawford and Evans, 2012, p.801). Alongside the public, the private and the voluntary, came increasingly the commercial. The pervasive movement of commercial security into 'new social spaces' (Manning, 2000) – such as cyberspace – has formed part of the second dimension of the shift in responsibility from State to citizen (Loader and Sparks, 2002). Within the wider picture since the mid-1990s, one of the effects of increasing globalisation has been the radical erosion of distinctions between internal and external security, war and crime,

[7] Also known as Neo-Classicism. The term 'Right Realism' was coined by Jock Young, arguably the prime mover behind the emergence of Left Realism.

the police and the military. Greatly adding to this have been the seismic shifts in the terrain of crime, national (in)security and governance caused by the 9/11 disaster and subsequent acts of terrorism. The mid-1990s also marked the beginning of the 'Internet Age' when, in 1994, the web was delivered to the masses via the internet. Since then, much of the web's profound influence on late modern society has been in bringing the global to the local, including crime.

In 2008, a global financial crisis triggered global recession. In addition to its dramatic impact on the public (and private) purse, that recession has brought real change in public opinion, a backlash which has included Banker-bashing and an even deeper distrust of politicians, individually[8] and collectively[9]. In turn, this has also led people to contest the policy of risk management which has been so dominant in recent times. From 2010-15 in Britain, a coalition government worked together in the wake of that recession. Within this governing alliance, ideological tension brought increasing political strain. Yet, over time, the responsibilisation rhetoric of the Conservatives held sway, reflected in policies such as the welfare-to-work programme and the 'Bedroom Tax.' Since 2015, that emphasis on responsibilisation has remained strong during two successive Conservative governments.

Today, set within the wider contexts of national security and of austerity in response to recession, the fight against cybercrime features ever-stronger messages of responsibilisation. Contributing to that potency and pressure is the fact that victims of cybercrime are often also unwitting accomplices to further crime. Victimhood can be initial, onward and ongoing. In the worst cases, this brings advanced, persistent threats to (national) cyber security. But, as the clamour for responsibilisation within cyber security grows, so too does the risk of 'victim blaming.'

### 2.2.1 Victim Blaming

Victim blaming occurs where businesses and/or people are *unjustly* held responsible (wholly or partially) for falling victim to crime. In other words, it involves 'unduly attributing victims' plights to their thoughts, characters or actions' (Harber *et al.*, 2015, p.603).

[8] For example, the expenses scandal, which began in May 2009.

[9] Reasons include the last Labour government's scant regulation of the Banking sector and, more recently, revelations about widespread, intrusive surveillance of citizens by government agencies (information that was whistle-blown by former National Security Agency employee Edward Snowden in June 2013).

My research seeks to further inform the discourses and practices concerning cybercrime victimisation and cyber security in the UK. To do this, it has cast a critical eye over the theoretical foundations of current policy in these areas. This means that it is situated also within the discipline of Victimology, which itself has developed during the aforementioned 50-year period of profound societal change. Specifically, I have investigated these issues from the perspective of Critical Victimology. Here, it is important to place Critical Victimology within the history of Victimology, and to compare it with Positivist Victimology, a victimological school of thought which has been criticised for facilitating victim blaming.

Victimology's essential focus is on the issue of victimisation, partly as another way of measuring crime and partly to better understand its impact (Newburn, 2013). Yet, setting a framework for victimology also demands the disentanglement of academic thinking and activist concerns (Mawby and Walklate, 1994), which is no simple matter (Fattah, 1989). To that end, three tendencies within victimological debate have been identified: the conservative, the liberal, and the radical-critical (Karmen, 1990). The defining traits of the conservative tendency include its concern to render people accountable for their actions, the encouragement of self-reliance, and notions of retributive justice (Karmen, 1990). Such Positivist Victimological thought has influenced greatly the policy discourses on crime prevention in general, and the issue of citizen responsibilisation in particular, bringing with it the aforementioned danger of victim blaming.

### 2.3 Positivist Victimology

Positivist Victimology itself has been the subject of much labelling. In addition to being termed Conservative Victimology (Karmen, 1990), it has also been referred to as Conventional Victimology (Walklate, 1989), Penal Victimology (Holyst, 1982) and Interactionist Victimology (Van Dijk, 1997). However, its defining characteristics remain unchanged. These include the discovery of factors which influence a non-random pattern of victimisation, and the examination of how victims contribute to their own victimisation (Miers, 1989; Spalek, 2006.). The early work within this field, which focused on the attributes of victims themselves (Von Hentig, 1948; Mendelsohn, 1956), together with later work which developed that theme through the notion of 'victim precipitation' (Wolfgang, 1958; Amir, 1971), has proven controversial. These approaches have been criticised for imputing blame and

responsibility to victims (Mawby and Walklate, 1994) through viewing their actions wrongly in terms of culpability (Kelly, 1988; Stanko, 1990). In response to such criticism, it has been argued that research into victims' roles in their victimisation is concerned, not with victim blaming, but with discovering why certain people fall victim to crime (Fattah, 1989). Often, however, 'there seems to be a thin line between blame and account, especially within discourses that emphasise the duty of citizens to avoid victimisation' (Spalek, 2006, p.35). Today, it may be the case that just such an emphasis continues to feature within government discourse on cyber security in the UK.

Controversy also pervades the issue of risk, and its management. Much of the analysis has focused on risk as an objective set of defensive procedures used to minimise criminal harm (O'Malley, 2006). But the experience and valuation of risk is subjective. Also, historically within Criminology 'there has been an implicit acceptance of the idea of risk as a forensic concept' (Walklate, 1997, p.37). Such assumptions have distracted the analytical gaze from risk's diversity (O'Malley, 2006) and narrowed the parameters of the criminological debate on the relationship between risk and criminal victimisation (Walklate, 1997).

Also in the Positivist tradition, there remains a body of work which focuses on patterns of victimisation and their use in crime prevention or reduction. It is comprised of two, similar approaches: Lifestyle Theory (Hindelang *et al.*, 1978) and Routine Activity Theory (Cohen and Felson, 1979) – hereafter referred to together as LRAT. Each focuses on the temporal and spatial convergence of offenders and victims (Gottfredson, 1981). One of the general criticisms of LRAT is its underlying assumption that we are all rational actors (Eigenberg and Garland, 2008). For example, it has been argued that it is not unusual for individuals to make decisions which are not overtly in their own best interests, perhaps because they may not be in a position to truly evaluate particular courses of action (Tunnell, 1992). It has also been criticised for failing to take sufficient account of the structural conditions within which decision-making takes place (Tilley and Laycock, 2002). My own research is concerned, *inter alia*, to identify the forces and factors which truly influence people's behaviour around cyber security within their everyday working lives. As I will later discuss at length, potentially there are factors other than self-interest at play which determine an individual's choices and patterns of behaviour.

The particular applicability of LRAT to cybercrime has been the subject of disagreement. Some have taken the view that it could be productive (Grabosky, 2001; Newman and Clarke, 2003; Taylor *et al.*, 2006), while others have argued that its worth is limited within the 'chronically spatio-temporally disorganised' environment of cyberspace (Yar, 2005). More specifically, Majid Yar has argued that, for several reasons, LRAT cannot be applied usefully to cyberspace: Firstly because, in contrast to physical spaces, virtual spaces can be transient and unstable (Yar, 2005)[10]. Secondly, because the temporal dimensions of cyberspace give less pattern to the interactions between offenders and victims (Ibid). And lastly, because those interactions are often asynchronous, and conducted at great physical distance between the two (Ibid). On this last point, although a Cyberlifestyle-Routine Activities Theory has since been developed, conceptualising the convergence of offenders and victims as occurring through the system of networked devices that constitute the internet (Reyns *et al.*, 2011), empirical tests of this new theory have used similar measurements to previous routine activity tests and 'have not led to improved evaluations of the theory' (Holt and Bossler, 2016, p.69).

Although research has illustrated that some of the basic constructs of LRAT may apply to cybercrime (Choi, 2008; Marcum, 2008; Holt and Bossler, 2009; Bossler and Holt, 2009; Ngo and Paternoster, 2011; Reyns *et al.*, 2011; Van Wilsem, 2011, 2013a), the majority of studies have tended to focus upon online harassment and cyberstalking victimisation, and have often been based on student populations. Overall, they are said to have delivered mixed results (Holt and Bossler, 2016, p.69), and have provided 'modest, though not always consistent, support for the utility of LRAT in understanding the risks of victimisation in cyberspace' (Ngo and Paternoster, 2011, p.776). Mixed results have also been seen to emerge from research into the more specific issue of the association between capable guardianship[11] and cybercrime victimisation (Holt and Bossler, 2014; Holt and Bossler, 2016).

Thus far, there has been limited research into the applicability of LRAT to online fraud and theft victimisation (Holt and Turner, 2012; Van Wilsem, 2013b; Reyns, 2013), but

[10] However, in response, it has also been pointed out that the online networks of a number of organisations (e.g. government agencies, universities and corporations) have a considerable degree of permanence and stability (Maimon *et al.*, 2015).

[11] Whether that be physical guardianship (e.g. use of computer security software) or social guardianship (e.g. computer skill levels), or both.

somewhat more research into malware infection victimisation (Szor, 2005; Wolfe *et al.*, 2008; Bossler and Holt, 2009; Holt and Copes, 2010; Holt and Turner, 2012; Holt and Bossler, 2013). Again, the results have been mixed, but the evidence suggests that some behaviours may affect the risk of victimisation (e.g. pirating media or viewing pornography online), and that the presence and use of protective software may reduce the likelihood of infection.

To date, it seems that LRAT is not particularly effective in explaining a diverse set of cybercrime victimisations (Ngo and Paternoster, 2011), and so it remains unclear whether LRAT can be used to explain (certain types of) cybercrimes (Leukefeldt and Yar, 2016). However, the theory has been somewhat successful in examining person-centred cybercrimes, such as online harassment and cyberstalking (Holt and Bossler, 2016). But it has been conceded that 'a great deal of future research [will be needed] in order to validate [any] notion that behaviour is more significant than demographics in the general risk of online victimisation' (Holt and Bossler, 2014, p.26). Interestingly, on the issue of suitable targets (within LRAT), one of the older research studies concluded that 'there may be no gender, age or race differences in target attractiveness relative to the risk of malware, since computers and their contents are the primary targets, not the individuals' (Bossler and Holt, 2009). However, much malware infection is now initiated through social engineering techniques – for instance, within the continuing rise in Ransomware attacks. As technological defences have grown stronger, cybercriminals have focused increasingly on exploiting human weakness as a means to their criminal ends (MacEwan, 2013; Chang *et al.*, 2013). Such attacks are aimed at differing types and levels of employee working within organisations[12].

Positivist Victimology has been criticised for failing to seek out, and then question, any structural factors which increase the risk of victimisation. More specifically, LRAT is said to provide only a partial analysis of human action and structural constraints within victimisation (Mawby and Walklate, 1994). By viewing victimisation through the narrowed lens of changeable lifestyle and routine activity choices, it also implicitly blames the victim for their plight, particularly where crime prevention strategies emerge from the notion of repeat victimisation (Walklate, 1992). The cyber security

[12] For instance, through 'spear phishing' and 'whaling' emails.

of small businesses is a setting in which that danger of victim blaming lurks when matters are viewed from such Positivist Victimological perspectives. Instead, my research has been conducted from the perspective of Critical Victimology.

### 2.4 Critical Victimology

While Positivist Victimology views victims either as passive or as responsible for the crimes committed against them, Critical Victimology advocates a more sophisticated analysis of how individual action is constructed and reconstructed within material conditions (Walklate, 1992; Spalek, 2006). This necessitates taking account of:

> 'individuals' conscious and unconscious activity, the structural processes which form the background to [such] activity, and the intended and unintended consequences of action which may change the conditions in which people act' (Spalek, 2006, p.44).

This then produces a clearer picture of how people act within, and resist, the structural conditions of their life (Mawby and Walklate, 1994). Critical Victimology is organised around three key concepts: Rights, Citizenship and the State. It works from the presumption that victims' rights are a crucial basis for future policy-making, which also implies a conception of citizenship that goes beyond a limiting emphasis on responsibility rather than rights (Mawby and Walklate, 1994). It takes account of the many connections between victimisation and political, economic and social processes (Spalek, 2006). Close critical analysis of government discourse on cybercrime victimisation and cyber security have been important aspects of my research, together with a focus on the power of social processes to influence individual behaviour towards cyber security rules.

The main focus of Critical Victimology has been on victim status, and how this is given, denied or rejected through the process of labelling. More specifically, the two key questions for Critical Victimology are: Who has the power to apply the victim label, and what considerations are significant in that determination? (Miers, 1990). Traditional discourses, such as those stemming from Positivist theory, have tended towards victim blaming (Rock, 2007). Through its analysis of current and recent discourses on cyber security, my research has sought to determine whether such victim blaming has been occurring.

One of the key issues that I have been investigating is the construction of the 'victim.' Within governmental, corporate and media discourse, the concept of 'victimhood' can be misleading. Often, it is portrayed, through stereotype, as being simple and clear-cut. In reality, it is far more complex (Fattah, 1991; Christie, 1986). That complexity stems from 'victimhood' being contingent upon intricate psychological, social and political processes, and 'its construction helping to determine which forms of victimisation, and what kinds of people, are helped' (Spalek, 2006. P.31).

To make someone responsible for something is to give them a duty towards it. To hold someone responsible for something is to regard them as accountable, answerable or culpable for it (Oxford English Dictionary, 2016). Responsibilisation accommodates both of these approaches. In itself, that is not contentious. However, controversy comes from Neoliberalism's embrace of the victim/offender dichotomy, and with it the concept of the 'ideal victim' (Christie, 1986). Politics have influenced heavily the knowledge and understanding of 'victimhood,' rooting it firmly in notions of vulnerability (Walklate, 2011; Donoghue, 2013; McAlinden, 2014). Consequently, there exists a 'hierarchy of victim legitimacy' (Walklate, 2011), atop of which sits that 'ideal victim.' This is a person who 'when hit by crime, most readily is given the complete and legitimate status of being a victim' (Christie, 1986, p.18). Stereotypically, they are weak, respectable, law-abiding, blameless and have sufficient power, influence or sympathy to gain victim status without threatening vested interests (Christie, 1986). Recognition of this stereotype is very useful in understanding victimhood, and in deconstructing public portrayals of it, especially 'when the idea of the victim is being used to promote or defend some criminal justice or penal policy' (Newburn, 2013, p.354).

During the last few years, the threat landscape has changed in significant ways. The lines between 'home' and 'work' have continued to blur, and citizens'/employees' use of cyberspace has both increased and become truly mobile (smartphones, smartwatches, tablets, laptops, cloud computing, the use of file-sharing Apps, and social media). These changes have come within, and across, their working and personal lives. Such developments, coupled with the dramatic rise in Bring Your Own Device (BYOD) and Bring Your Own Service (BYOS) work practices, deliver additional cyber security difficulties and risks (Romer, 2014), and further complicate the responsibilisation of citizens/employees.

The threat posed by non-malicious insiders[13] to the information/cyber security of organisations remains the subject of regular, ongoing research (e.g. CERT, 2016; Verizon, 2017). However, within that corpus there has been little research into the information technology practices and perceptions of online risk in, and extending from, the workplace. To date, the most extensive piece of research on this matter in that specific area[14] has been an international study of 3250 office workers, conducted over a two-week period via the use of a questionnaire[15] (LMRC, 2010). The results of this study confirmed, *inter alia*, that large amounts of data were circulating outside work-based systems in a number of different formats[16], that these employees were prepared to take risks (especially where they thought it appropriate to do so), and that they were using network technologies quite intensively – especially, social networking to increase their professional, as well as social, contacts (Wall, 2013, p.114). However, this research was done some time ago now (in September 2010), and was not conducted solely within the UK[17]. Also, since then advances in web and internet technologies have further changed the experiences and practices of people within their personal and working lives. My own research is the first to provide a Critical Victimological insight into the everyday cyber security experiences, attitudes, habits and practices of employees within small businesses in the UK.

Previously, there has been very little research into cybercrime conducted from a Critical Victimological perspective. However, several pieces of work do fall into this category – if only, because they made mention of Neoliberal responsibilisation and victim blaming within an online setting. Respectively, that research was conducted in America (Monahan, 2009), Canada (Whitson and Haggerty, 2008) and Australia (Cross, 2013). However, the first two pieces of research focused exclusively on Identity Theft,

[13] Categorised further into 'negligent insiders' and 'well-meaning insiders' (Wall, 2013).
[14] Note that the issues of employees' IT practices and their perceptions of online risk have also featured within other corpuses of research, such as information/cyber security awareness and information/cyber security policy compliance. These will be considered later on this chapter, during discussion of the more specific matters of training employees in cyber security, and their behaviour towards policy rules concerning cyber security.
[15] Note that only the questionnaire results were published, and only temporarily. They have since been withdrawn from public scrutiny (by the organisation which paid a market research company to conduct the survey). However, the results have since been discussed in detail within a journal article – see Wall (2013).
[16] For instance, 71 per cent of the workers had emailed work documents to their private email addresses (to work on them outside their employers' premises), and 42 per cent had copied work to non-encrypted or non-protected USB sticks (LMRMC, 2010, quoted in Wall, 2013).
[17] Fewer than a third of the research participants worked in offices within the UK. The others participants worked for organisations situated in Canada, Hungary, Poland, South Africa and the USA.

and gave consideration to both online and offline forms of that crime. Also, they were concerned essentially with individual vigilance in the management of personal data. The third, more recent piece of research explored the victim blaming discourse surrounding online fraud, premised heavily on the notion of individual greed. It challenged that discourse, arguing that it does not take into account the level of deception and the targeting of vulnerability that is employed by perpetrators of that type of crime. However, this research was focused exclusively on cyber fraud that was initiated through phishing emails and was targeting 'seniors' (victims aged 50 years or older).

Potentially then, responsibilisation can complicate the claiming of victim status, and very different consequences may flow from the presence or absence of that status. Gain of it can attract support (personal, social, financial, commercial, legal). Lack of it can attract criticism and liability (personal, social, financial, commercial, legal). The *nature* of the responsibilisation itself seems to determine this: the perspective from which it is done (and by whom), its manner, tone and degree. A key part of my research has been critical analysis of government discourse on cybercrime victimisation and cyber security. I have also scrutinised some near-government and corporate discourse on these matters, particularly within the SME sector of UK business. An important part of all that analysis has been the identification of pressures – social, economic, political, legal, national and global – which influence and determine the content and tone of such discourses in the UK. Alongside this deconstruction, I have been examining whether use of the 'ideal victim' stereotype is reinforced by the very nature of cyberspace, and how this influences behaviour within it. Such critical analysis of all these connected matters has not been done before.

### 2.5 Further ambient pressures

While exploring the potential dangers which can flow from such constructions and discourses, I also looked at additional pressures that shape perceptions, opinions and policies within UK cyber security. Chief among these is the previously mentioned fact that within much cybercrime victimhood feeds further criminality (in degree, range and type), so that many instances of cybercrime victimisation can be initial, ongoing and onward. This hardens the responsibilisation rhetoric from government down to (and between) businesses, and on to employees. Within the general picture of late modern 'existential anxiety' (Giddens, 1990; Bauman, 2006), more particular risks are

perceived by each of these parties: The government fears breaches of national cyber security, with consequences which could include loss of political office. Businesses fear falling victim to cyber attack, with consequences which could include reputational damage and financial loss, together with potential legal liability for passing victimhood on to other businesses and individuals. Employees fear blame and sanction if their employer holds them ultimately responsible for cyber security breaches. Such sanction could be extra-legal, such as 'shaming' in the workplace (Furnell, 2012; Wall, 2013), or legal, such as termination of employment. The potential for victim blaming and scapegoating, fuelled by the power to refuse victim status, is clear.

There is also the potential for regulatory creep, based around arguments of 'victim facilitation' which claim that in some way(s) the victim has made themself an easier target for criminality. For example, the creation of a legal duty of vigilance towards cybercrime – with liability possibly extending to complicity in the victimisation of others – has already been advocated (Brenner, 2004; Jewkes, 2007). Such ideas could return to the political/legal forum. Also, the issue of cyber insurance has been looming larger, driven on and supported by the government[18] (Cabinet Office, 2014a). Currently, it seems that many businesses are reluctant to purchase cyber insurance because of the cost, and too many exclusions/restrictions and uninsurable risks (Experian, 2013; Alloway and Kurcher, 2014); and that reluctance is strongest within small businesses (Cabinet Office, 2015a). However, as that market continues to mature, the pressure for businesses to take up cyber insurance will intensify. Globally, the cyber insurance market in 2017 has an estimated worth of $3.5 billion, and this is predicted to double by 2020 (BBC News, 2017). Increasingly then, cyber insurance companies will join the actuarial fray of risk management and victim-labelling, further complicating and contorting it.

Also on the horizon is the prospect that businesses in the UK will be required by law to report certain incidents of cybercrime. For example, in 2013 a Parliamentary Select Committee recommended that banks should have to report all online fraud to the police, including logged details of where the attacks emanate from (House of Commons Home Affairs Committee, 2013). There has also been political discussion of

[18] In 2014, the government announced its intention to support the growth of a cyber insurance market in the UK, and set up industry-chaired working groups to consider 'how best to use insurance as a driver for improving cyber security practice in UK businesses, and SMEs in particular' (Cabinet Office, 2014).

a need to consult on the creation of a legal requirement for all private companies to report serious cyber attacks which threaten the UK's national infrastructure (Sparkes, 2014). Also, of course, while it continues to negotiate the UK's exit from the European Union, the government is planning to create cyber security and data protection laws which implement faithfully the provisions of the EU's Network and Information Security Directive 2016 (NISD) and resemble closely the provisions of its forthcoming General Data Protection Regulation 2018 (GDPR). Necessarily, this will be done to avoid trade barriers with the EU, post-Brexit. Respectively, those new laws will impose duties upon businesses to report certain types of cyber security incident (NISD), including data breaches (GDPR), in certain circumstances, to the relevant authorities; and those watchdogs will have been given much sharper teeth[19]. All of these movements and measures will simply add to the aforementioned pressures being felt by businesses in the UK, particularly SMEs.

In consideration of all these aforementioned matters, the first question that my research has been investigating is:

> In the UK, is government discourse responsibilising small businesses, and the people who work in them, for cyber security? If so, how? And with what implications?

### 2.6 The use of training and rules in the governance of behaviour concerning cyber security

All organisations, small businesses included, are socio-technical systems, and so efforts to keep them secure must address both technical *and* human aspects (Sasse and Flechais, 2005). Indeed, people's co-operation plays a critical role within organisational security (Beautement *et al.*, 2016). My research has been concerned with people's behaviour around cyber security. More specifically, it has been investigating the challenges which lie within the guidance and governance of that behaviour through training, and through the use of policy rules.

[19] For example, in cases of serious failures, the GDPR gives to each Member State's supervisory authority the power to impose fines of up to €20 million (£18 million), or 4 % of an organisation's annual turnover, whichever is the greater – Art.83, GDPR.

### 2.6.1 Shaping people's behaviour through training

Recently, the government reported a dearth of cyber security training within the business sector, complaining that:

> 'In businesses, many staff members are not cyber security aware and do not understand their responsibilities in this regard, partially due to a lack of formal training' (HM Government, 2016b, p.22).

Indeed, during its latest annual cyber security survey, the government found that within only 20% of businesses had staff attended any form of cyber security training during the previous year (HM Government, 2017, p.2). Furthermore, it is claimed that 'most organisations that deliver cyber security training to their staff do it on an occasional and irregular basis' (Caldwell, 2016, p.12).

Good communication between an organisation and its staff is one of the key elements to cyber security (Adams and Sasse, 1999). The two main goals of cyber security training are to influence people's attitudes towards cyber security and to motivate them into cyber-secure practices. Previous research has stressed the importance of educating staff, claiming that it makes them aware of the consequences of their actions and shows them the dangers that can result from insecure behaviour (Besnard and Arief, 2004; Parsons *et al.*, 2010). However, there is evidence that security awareness training activities have not been very effective. For example, an Information Security Forum survey found that, while 75% of ISF Members had an ongoing awareness program, 'only 15% reported that they had reached the heightened level of awareness and positive behaviours that they were striving for' (Information Security Forum, 2014). Also, opinions differ on whether such training provides value for money. Some consider it the most cost-effective form of security control (Abawayjy, 2014; Albrechtsen and Hovden, 2010), while others think that, typically, it is an expensive and time-consuming approach (Busch *et al.*, 2016). My own research makes a contribution to this debate because, *inter alia*, it has explored the financial pressures and competing priorities that shape decisions on whether, to what extent, and in what form *small businesses* provide cyber security training to their employees. Also, of course, such decision-making sits within that wider context of responsibilisation, in which the government continues to demand that *all* businesses train their staff in cyber security.

Next, mention must be made of the 'compliance budget' (Beautement *et al.*, 2008). Here, 'compliance' means choosing to behave in a way required by the organisation that employs you, even though that behaviour may hinder you in meeting your own work goals. Each employee's budget is limited, and in each instance they weigh up the costs and benefits of a security measure or procedure against its perceived cost to them in terms of the extra (non-productive) effort that it demands (Beautement and Sasse, 2009). Particular mention is made of this here because – beyond that internal cost/benefit analysis – training is one of the external factors which can influence the size of a person's own compliance budget, or the rate at which it becomes spent (Beautement *et al.*, 2008). Also, crucially, the amount by which a person's compliance budget can be increased through training is limited as well (Ibid).

Certainly, previous research has found that *effective* training in information/cyber security can improve individual performance, and thereby reduce the cost associated with security measures (Beautement *et al.*, 2008). Indeed, by increasing their competence, it can build people's confidence in using such measures – which is a benefit to them, and to the organisation (Ibid). Also, by raising in them an awareness of the dangers faced by the organisation, it increases the perceived benefits of compliance (Ibid). However, my research explores specifically the challenges and barriers to the provision of effective cyber security training within *small businesses* in the UK, and has been conducted within businesses from three different business sectors (marketing, legal, and charitable).

Also, my investigations connect with, or add to, existing research on more specific matters, such as 'security fatigue' (Furnell and Thomson, 2009a; Stanton *et al.*, 2016). This is where people tire of security procedures and processes, often because of the aforementioned 'friction' with their primary work tasks, caused by an imbalance between security and usability (Beautement *et al.*, 2008; Bada and Sasse, 2014).

My work also adds to existing research on people's preferences for training delivery methods, and the efficacy of those methods. In particular, it contributes more findings on employees' views about classroom-based delivery and online delivery of cyber security training. Previous research has shown that people often express a preference for classroom-based delivery, but that this model also has its own drawbacks (Abawajy, 2014). Firstly, its success is often dependent on the ability of the instructor to engage the audience (Cone *et al.*, 2007). Also, when not designed

carefully, such training can be rather 'static' (Valentine, 2006) and based on rote learning, which does not ask trainees to think about and apply cyber security concepts (Cone *et al.*, 2007; Abawajy, 2014). However, other research suggests that participative group sessions – characterised by interaction and collective dialogue, including the sharing of experiences and knowledge – is more likely to be successful (Albrechtesen and Hovden, 2010; Abawajy, 2014); however, this approach can itself be somewhat dependent on the amount of pre-existing knowledge among the participants on matters of cyber security (Abawajy, 2014).

Online delivery methods come in different forms. These include blogging, which can potentially be quite effective (Kumaraguru *et al.*, 2007), and mobile learning platforms, which deliver flexible learning at a pace chosen by each individual, but can also afford minimal engagement (Cone *et al.*, 2007). In previous research, email has been considered a useful way of doing this (Wilson and Hash, 2003), partly because it is less costly, flexible and (potentially) has extensive reach. However, such emails can get 'lost' (i.e. deprioritised or ignored) within the increasing volume of emails that people receive each day (Abawajy, 2014).

My research has included the application of a theory called Meaning Finitism. This theory will be explained fully later on in this chapter (in section 2.7.1). However, mention of it is made here because it brings crucial insight to the subject of training (as well as rule-following). Meaning Finitism argues that there are three key aspects of any training process:

> 'First, no matter how many examples the teacher gives to the student, the number will always be *finite*. Second, the number of future instances of term use will, in effect, be *infinite*; no immutable limit restricts how many uses can or will occur. Third, no two objects or instances of use will be identical' [emphasis in original] (Schyfter, 2016, p.313).

Together, these bring the 'eradicable problem' (Bloor, 1997) that the training itself cannot guarantee which next step the trainee will later take, as they encounter each new instance of its use. This is because 'meanings, definitions and instructions are generalised, and instances of use are particular' (Schyfter, 2016, p.313). In short, training cannot ensure that the trainee's next steps are the ones envisaged by the trainer. However, if a Finitist approach is taken to training, such correlation will be

much more likely to occur. This involves the use of certain case study methods, which provide a framing technique from the ground upwards. These training methods will be discussed in detail later on (in section 2.7.3).

In consideration of all these additional matters, the second question that my research has been investigating is:

> Within their everyday working lives, do employees within small businesses practice what their government and their employers preach to them about cyber security? And if not, why not?

### 2.6.2 Governing people's behaviour through policy rules

There exists already a large body of research on information/cyber security policy compliance. Much of it has involved the application of behavioral theories to identify the influences upon people's behaviour around this matter. It has included the use of Protection Motivation Theory (e.g. Herath and Rao, 2009a; Vance *et al.*, 2012), the Theory of Planned Behaviour (e.g. Ifinedo, 2012) and Rational Choice Theory (e.g. Bulgurcu *et al.*, 2010; Vance and Siponen, 2012). Factors that have been found to influence security compliance include: **attitude** (Pahnila *et al.*, 2007; Herath and Rao, 2009; Bulgurcu *et al.*, 2010; Ifinedo, 2014), **self-efficacy** (Rhee *et al.*, 2009; Herath and Rao, 2009a; Johnston and Warkentin, 2010; Bulgurcu *et al.*, 2010; Ifinedo 2012, 2014; Vance *et al.*, 2012; Dang-Pham and Pittayachawan, 2015), **the cost(s) of compliance**[20] (Leach, 2003; Adams and Blandford, 2005; Beautement *et al.*, 2008; Furnell and Rajendran, 2012; D'Arcy *et al.*, 2014), **fear of security threats** (Ifinedo, 2012; Vance *et al.*, 2012; Dang-Pham and Pittayachawan, 2015) **and perceptions on the likelihood of their occurrence** (Lee *et al.*, 2008; Ifinedo, 2012; Siponen *et al.*, 2014) , **and the severity of their consequences**[21] (Pahnila *et al.*, 2007; Herath and Rao, 2009a; Vance *et al.*, 2012; Siponen *et al.*, 2014).

Recent research has begun to show that this matter is yet more complicated, because security behaviours are motivated by different factors and to differing degrees (Blythe *et al.*, 2015). My own research also makes an important contribution to that developing line of research, in particular by its exploration of the relation between

[20] However, note also negative results from Herath and Rao, 2009a and Vance *et al.*, 2012.
[21] However, not also negative results from Ifinedo, 2012.

rules and conduct, and the factors which influence rule-following behaviour around cyber security within everyday work (see section 2.7 below).

Much of the previous research has approached the matter of compliance from individualist, psychological perspectives. However, social influences have been found to affect compliance as well (Herath and Rao, 2009, 2009a; Bulgurcu *et al.*, 2010; Ifinedo, 2012, 2014). More specifically, for example, normative expectations and social pressure ('subjective norms') driving people's intentions to behave in security-compliant ways (Ajzen, 1991; Herath and Rao, 2009). Alongside some focus on the individual and the psychological, my own research has been conducted mainly from collectivist, sociological perspectives. Indeed, it has involved the use of theoretical thinking from other disciplines never before applied within the subject of information/cyber security. By doing so, it has demonstrated that responsibilising employees for cyber security – and guiding and governing their behaviour as part of that – is even more complicated than researchers, employers and the government have previously thought. These newly-applied theories will now be discussed in detail within the next section.

### 2.7 Rules, and rule-following behaviour

Traditionally, the relation of theory to practice has been defined in one of two main ways. The first ('rationalist') approach accords priority to theory over practice, and the second ('conservative') approach accords priority to practice over theory (Oakeshott, 1975; Bloor, 2001; Barnes, 2001; Schatzki, 2001). Rule-following *seems* like a case of the former, in which 'propositional content and meaning precede and determine the action of following the rule' (Bloor, 2001, p.95). But is this really so? Focussing on behaviour towards rules concerning cyber security, my own research addresses some key questions about what rules are, and what they can and cannot achieve, as well as how and why practice can differ from theory (i.e. the rules). This has involved the application of a sociological theory (Rule Scepticism) which itself is an interpretation of philosophical thinking (Wittgenstein) and theory (Meaning Finitism) on the subject of rules and rule-following – something that has not been done before within the context of information/cyber security.

### 2.7.1 Meaning Finitism

By holding that the meaning of a concept is to be understood through its use, the philosopher Ludwig Wittgenstein is said to have won back rule-following for the conservative tradition (Bloor, 2001, p.96). Giving priority to practice over theory[22], he insisted that we should use only naturalistic resources for the understanding of rule-following (Wittgenstein, 1967, p.25; Bloor, 2001, p.96). Throughout much of his discussion of rules, Wittgenstein wrestled with the question of what ensures that someone's next step will be the one required by the rule (Sharrock, 2004; Wittgenstein, 1967, 1967a, 1969 and 1978). He argued that the expression of a rule cannot exhaustively define or otherwise control its contextual application, because rules themselves, and the teaching of them, can feature only a *finite* number of examples and illustrations. Given this, he recognised that the problem of 'taking the next step' is always with us, both in *learning* and *using* rules (Bloor, 1997; Wittgenstein, 1978). Each involves moving from known to new cases. This is because, while some rules are finite (e.g. learning the alphabet), many are not (e.g. learning not to engage with suspicious emails). Consequently, we must always go beyond the given examples, or be deemed capable of doing so, before we can be said to have learned the rule that is being taught to us (Bloor, 1997). The same problem arises in the actual *use* of such rules. A rule is applied to the next case by analogy with existing ones (Wittgenstein, 1967; Barnes, Bloor and Henry, 1996), but analogies, and analogical reasoning, can always be contested (Hatherly *et al.*, 2005).

So, Wittgenstein rejected the notion that our use of a rule is determined by the meaning that we have grasped from the language of the rule. Replacing that deterministic picture with one that emphasises the *practical* basis of rule-following, he argued that meaning does not pre-exist in the rules; rather, people *generate* meaning as they *go along*, moving from past to new instances of rule application. So, there is nothing fully formed in the present that is capable of distinguishing *in advance* all the things to which a rule will be correctly applicable (Barnes *et al.*, 1996). In this way, Meaning Finitism links to Meaning Scepticism: It is precisely *because* future applications of a rule cannot be pre-determined that there is no (private, mentalistic)

[22] Note that practice is now frequently identified as 'the primary generic social thing' (Schatzki, 2001); or indeed, 'the only social thing' (Barnes, 2001).

fact of what a rule means. In short, as Wittgenstein put it, 'meaning is use' (Wittgenstein, 1967). By this he meant that meaning does not *explain* use, it *comes* from use; and *correct* use is defined by normative standards set and maintained by consensus within the group of interacting rule-followers. It is their consensus that renders those norms objective, 'a source of external and impersonal constraint on the individual' (Bloor, 1997, p.17). In this way, correct use follows from how individuals employ terms and concepts *within the social collective* to which they belong (Schyfter, 2016).

For example, into its staff handbook a business places a new written rule which states that: 'Employees must log out of their work PCs whenever they are away from their desks.' During a staff meeting, and later also via email, all of the employees are notified of this new rule and told to follow it from the next day forward. During the course of that next day, while trying to follow this new rule, most of the employees find that they are logging in and out of their work PCs many times. This both delays and annoys them. Gradually, they 'decide' *collectively* – through spoken and unspoken codes of practice – that the rule should *not* be interpreted to mean that employees must log off *every single time* they are physically away from their desks. Instead, a set of 'agreed' practices begin to emerge that are considered 'correct' applications of the rule (i.e. successful acts of rule-following):

- No need to log off when you leave your desk to go to the toilet.
- No need to log off when you leave your desk to fetch a cup of water from the water cooler, or to make a cup of tea/coffee in the staff kitchen.
- Usually, only log off when know you are going to be away from your desk for more than 15 minutes.
- Where someone who works next to or near you agrees to keep an eye on your work station while you are away from it, the logging off rule need not be applied. But if that person leaves their work station before you return to yours, they must log you off from your PC before they leave the area.

In practice then, their individual behaviour is being shaped by their collective agreement that the rule is to be applied *in these ways*. On the ground, the rule is evolving with the practice, and the practice is evolving with the agreed applications of the rule. Meaning is coming from use (Wittgenstein, 1967; Bloor, 1997).

From outside the business, looking in – or from on high within the business, looking down – it will look like these employees are simply not following the rule. But that is because the observer[23] can see only the (literal wording of the) rule and the apparent disregard of it – but not the community consensus and patterns of practice that have built up over time. Crucially then, the observer's view is restricted. They cannot see, and understand, the *real* influences on this rule-following behaviour, and so may *take* the view that it is simply the result of negligence (or worse), and is therefore worthy of blame and sanction.

### 2.7.2 Rule Scepticism

Wittgenstein's reflections on rule-following have been debated at length. The two main sides to that debate have featured scepticist and antiscepticist readings of his discussion of the topic. Rule Scepticism takes Wittgenstein to be arguing that the relation between rules and conduct is indeterminate, and that social conventions and learned dispositions account for orderly actions (Lynch, 1992). Contrastingly, the antiscepticist position holds that Wittgenstein treats rules inseparably from practical conduct, so that there is no basis for explaining the relation between rules and conduct by invoking extrinsic factors (Ibid).

My own reading of Wittgenstein's thoughts on rule-following accords with the Rule Scepticist interpretation of his work. It takes him to be arguing that, in themselves, rules possess no agency (Bloor, 1997). Wittgenstein claimed that when we follow a rule, we do so 'blindly' (Wittgenstein, 1967: 219). By this he meant that the core basis of our actions is blind habit: 'This is simply what I do' (Wittgenstein, 1967: 217). The Rule Scepticist reading of this is that 'we act as we do because we are the sort of creature we are, and we have been trained to act in that way: that is all' (Bloor, 2001, p.96).

So, if it is not determined by rules alone, what shapes and limits our rule-following practice? Rule Scepticism looks beneath and beyond such practice to identify other sources of influence upon it. These include psychological dispositions, communal consensus and social conventions. Consequently, Rule Sceptics argue that:

[23] E.g. An industry regulator, an insurance company, the government, or the Chief Executive of the business itself.

> '[E]ach application of a rule is negotiable, and the negotiation (or lack of it) is intelligible in terms of the dispositions and interests of the rule followers themselves: that is where agency truly lies' (Bloor, 1992, p.271).

Therefore, it is not 'meaning' or 'logic' which prevents us from taking rules in any direction as we apply them. It is the 'down-to-earth contingencies' that surround us each time that we do so (Bloor, 1997, p.19-20).

But what determines whether our actions amount to *correct* rule-following? Rule Sceptics argue that Wittgenstein answered this by explaining that rule-following is a *practice* (Wittgenstein, 1967: 202), but a *shared* practice (Bloor, 1997); and so, the norms of rule-following are set and maintained by consensus within the community of rule followers, and form part of the 'currency of social interaction' (Bloor, 1997, p.100). Consequently, Rule Sceptics claim that Wittgenstein rightly saw rules and rule-following as *social processes*. However, while identifying and emphasising the potent influence that these communal forces have on rule-following behaviour, Rule Sceptics also recognise that those same forces cannot remove the indeterminacy of meaning: 'Consensus may furnish us with norms, but it does not overcome Finitism. Nothing can overcome Finitism' (Bloor, 1997, p.26).

Before going on to consider the issue of training within that permanent context of Finitism, a specific truth about breach of rules within Cyber/Information Security sector is worthy of mention here: This is that, in stark contrast to the Health & Safety sector – where rule-breaking would be regarded as a sign that a system is not working as intended, and that this requires investigation to determine why it happened and what changes should be made (e.g. transport 'near misses') – within the Cyber/Information Security sector the tendency is for nobody to ask why people are not following the rules, and for nothing to happen unless and until a breach occurs.

### 2.7.3 Finitism and training

The ever-presence of Meaning Finitism poses a real threat to the efficacy of training. But is there such a thing as a Finitist approach to training? Thomas Kuhn's work on the production of scientific knowledge (Kuhn, 1970), and its subsequent reformulation within the Sociology of Scientific Knowledge (Barnes, 1982), has produced a Finitist model of training that has been seen in other areas of education, such as Biomedicine (see, for instance, Sturdy, 2007) and Forensic Medical Examination (see Rees, 2011).

Kuhn viewed scientific knowledge in terms of successful puzzle-solving, and explained that such knowledge is produced by applying accepted examples of puzzle-solving to new empirical or theoretical puzzles (Kuhn, 1970). In this way, knowledge is generated on a case-by-case basis. According this view then, scientific knowledge is 'knowledge of cases' (Sturdy, 2007, p.676); more specifically, knowledge of what Kuhn termed 'exemplars.' These he defined as 'concrete problem solutions, accepted by the group as, in a quite usual sense, paradigmatic' (Kuhn, 1977, p.298). Kuhn realised that:

> 'Every new puzzle-situation inevitably differs from everything that has gone before, [and that] consequently, the business of exemplar-based puzzle-solving cannot proceed mechanically, through the unreflective application of predetermined methodological rules' (Sturdy, 2007 p.676).

In short, Kuhn recognised that the use of exemplars is 'a matter of inductive judgement rather than deductive reasoning' (Ibid). First, it involves an appraisal of the new case and previous cases. Then, the use of reasoning by analogy to identify any connection between them. And finally, an assessment of their levels of similarity, or 'similarity relations' (Kuhn, 1977; Barnes, 1982). Crucially, however, such judgements of similarity come, not from the mind of the individual, but from the collective mind of the community, and they are the subject of constant development and dissemination. In other words, these normative standards are produced:

> 'from the consensus generated by a number of interacting rule followers, [which] is maintained by collectively monitoring, controlling and sanctioning their individual tendencies' (Bloor, 1997, p.17).

Necessarily, new cases can and do bring change. Within any classificatory scheme, case types can be seen as knots upon a net (Barnes *et al.*, 1996; Bloor, 1998; Rees, 2011), the distance between them set by those similarity relations, and being repositioned as each new case is introduced (Rees, 2011).

Kuhn's own analysis came in part from his observations of the use of exemplars within the teaching of Physics. He noticed that students might claim to have understood a chapter within a Physics textbook, but then struggle when answering the end-of-chapter questions. However, he noticed also that when they repeated these exercises a number of times, they learned to use correctly the tools and concepts that they

were applying. In turn, this led to them becoming as acquainted with those tools and concepts as had other members of the Physics community. The important point here is that:

> 'these end-of-chapter exercises were not checks to identify whether the student had absorbed the meaning of the text; rather, it was only via their successful completion that the student mastered said concepts (Barnes, 1982; Warwick and Kaiser, 2005). In other words, the student's perception and cognition were disciplined through the exercise to conform to their peers' (Rees, 2011, p.868).

This form of training confronts the main weakness of what has been termed 'learning by ostension' (Kuhn, 1977; Barnes, 1982, Barnes *et al.*, 1996), in which the trainer introduces the trainee to a new term/case, tells them how it should be classified, and what inferences can be drawn from it. Therein, the problem is that 'no singular act of observation and description can teach the trainee the correct application/inference' (Rees, 2011, p.867). Certainly, more ostensive learning may increase the chances of a trainee making classifications that are deemed 'correct' by the community, but it will never deliver the ongoing competence in classification that is required. That can be gained only from continued observation and use of examples, exercises and exemplars – alongside, when needed, some correction and reiteration from the trainer – within the aforementioned Finitist approach to training; and it will be the community itself that will decide whether, and when, an individual has attained that competence (Barnes, 1981; Bloor, 1982). However, given that classification itself rests upon previous observation of a *finite* set of cases, there remains the potential for any new case to test the knowledge and skills of the 'competent' classifier.

Finitism shows us, not only that all of our classifications are judgements, but that they are social conventions as well. This is because the *community* decides what amounts to 'correct' classification, since 'there is no scale for the weighing of similarity against difference given in the nature of external reality' (Barnes, 1981, p.309). Necessarily, this also means that all classifications are revisable and that all classificatory terms, and applications of them, are interrelated (Barnes *et al.*, 1996).

## 2.8 Conclusion

My research has been concerned with the human aspects of cyber security. More specifically, with the responsibilisation of small business employees for cyber security within their everyday working lives. It has investigated this matter through two connected sets of research questions:

1. **In the UK, is government discourse responsibilising small businesses, and the people who work in them, for cyber security? If so, how? And with what implications?**

2. **Within their everyday working lives, do employees within small businesses practise what their government and their employers preach to them about cyber security? And if not, why not?**

In its investigation of these questions, this research has visited several disciplines of study other than Cyber Security and Information Security. These are Victimology, Sociology and Philosophy.

In some ways, my research contributes to existing bodies of research. For example, in producing more empirical data and further observations/reflections on cyber security training, and compliance with cyber security policies, within businesses in the UK. Indeed, it gives particular insight of those matters within small businesses (and across three small business sectors). However, my research also makes its own original contributions to academic research. It is the first to critically analyse UK government discourse on cyber security and cybercrime victimisation via the themes of (Neoliberal) responsibilisation and victim blaming. It is also provides the first insight into the everyday cyber security practices etc of small business employees in the UK from the perspective of Critical Victimology. And lastly, it is the first piece of research to apply the theories of Meaning Finitism and Rule Scepticism to questions about rules and rule-following concerning cyber security.

# Chapter 3: Research Methods

## 3.1 Introduction

In the previous chapter, I set out and explained my chosen research questions. In this chapter, I will discuss how I researched those questions. Mainly, this will involve outlining my chosen research methods and commenting on their use, but will also include some initial discussion of how I recruited the research participants.

All of the methods that I chose were qualitative; to answer my research questions, I neither intended nor needed to produce statistical analyses. My mixed-methods approach comprised the following:

- **Documentary Analysis** of governmental and corporate discourse on cybercrime victimisation and cyber security.
- An initial **Observation** of the physical, social and technological layout of the office-working environments at the three small businesses where I planned to gather data via the following two methods:
- A five-day **Diary Study**, conducted online.
- Followed up by semi-structured, one-to-one **Interviewing**.

Being mindful of practical considerations (e.g. the physical limits and ethical boundaries of constant observation), I thought that this particular mix of methods would best illuminate my research topic, and provide a range of data that would truly inform the Critical Victimological approach that I was taking. Different types of data 'can be, and often are, blended creatively and effectively' (Ritchie *et al.*, 2014, p.52), and Diary Study can be used effectively in combination with other methods in a variety of designs (Alaszewski, 2006). Although the classic combination is that of ethnographic observation with interviews (Seale, 2012), I thought that combining diary reports with interviews would work well in my chosen project. Later on, I will discuss in more detail my choice and use of these methods, but first I will explain how I recruited the research participants.

## 3.2 Recruitment

I predicted that it would not be easy to persuade businesses to take part in my research study, because they might be understandably cautious about allowing

someone else in to evaluate their cyber security regimes and practices. However, the fact that I was seeking to recruit just three small businesses brought with it a greater chance of success. It has been recognised that:

> 'Information security research is one of the most intrusive types of organisation research, and there is undoubtedly a general mistrust of any 'outsider' attempting to gain data…….Firms are unwilling to divulge such information without strong assurances that the information provided will in no way harm them, yet could provide insight into how to improve their organisation. Time is far better spent focusing on a few, select firms with whom the researcher has developed an excellent rapport and trust' (Kotulic and Clark, 2004, pp.604-605).

Ideally, I hoped to find three businesses that were similar in terms of their employees' use of technology, but different in the level and degree of their cyber security strategies and policies. Ultimately, I managed to achieve this mix of recruited organisations. Officially, I was not allowed to begin recruitment for my research project until it had received ethical approval from my Faculty's Ethics Committee. This was gained on 9th December 2014, and I began my recruitment drive the next day.

In total, I spent seven months on recruitment. By the beginning of July 2015, I had recruited the last of the three businesses that agreed to participate in my research. One of them (Business A) is a 'micro business,' and the other two (Businesses B and C) are 'small businesses'[24]. Deliberately, I had cast my recruitment net widely, inviting SMEs from the public, private and charitable sectors to take part in my research. In the main, my recruitment strategy had comprised three activities: 1) attending a number of events in Hampshire aimed at the SME community, at which I would give out copies of an advert for my research study[25], 2) sending a copy of that advert via email to many thousands of SMEs in England[26], and 3) speaking with personal contacts

[24] The UK government continues to define a 'micro business' as one which employs fewer than 10 people, a 'small business' as one which employees between 10 and 49 people, and a 'medium-sized business' as one which employs between 50 and 249 people (Ward and Rhodes, 2014, p.3).

[25] A copy of that advert can be found at Appendix J on page 238. Examples of the events that I attended include a 'Digital Summit' in Winchester (March 2015), a 'Cyber Security Cluster' at Chilworth Science Park near Southampton (April 2015) and an 'Open for Business' event at the University of Southampton (May 2015).

[26] I sought and gained the assistance of several organisations to achieve this. These included Hampshire County Council, the Federation of Small Businesses and the British Chamber of Commerce.

within the Hampshire business community. Ultimately, it was the last two of these activities that bore fruit. Two of the three recruited businesses responded to a mail-merged advert that I had sent out to 6000 SMEs in the Hampshire area (with the assistance of Hampshire County Council's Economic Development Department). I recruited the third business through a personal contact, who himself is a member of its Board of Trustees. Fortunately, the recruited businesses are in different business sectors, and this simply brought further scope for their comparison: Business A is an email marketing business, Business B is a law firm, and Business C is a charity. All three of these businesses are based in Hampshire.

With each of these businesses, I took care to build the aforementioned rapport (Kotulic and Clark, 2004) that is crucial to gaining and retaining their trust in the research project, and the researcher. This was achieved through several means. After initial email exchanges with them, I went to meet the people who had contacted me. Respectively, these were the owner of Business A, the IT Manager in Business B and the Chief Executive of Business C. At those meetings, I thanked them for their interest in my research project, and provided them with additional information about it, and myself. I was very open to any questions that they had, and gave them firm assurances that the businesses, the employees and the data collected from them would receive careful protection throughout and beyond the study (e.g. via anonymity and other data protection measures). I was also keen to stress the fact that I was an *independent* researcher, studying for an educational qualification within a University. I assured them that I was someone who would always be friendly and sensitive towards research participants. Last but not least, I reiterated that if they took part in the study they would receive a bespoke report on the cyber security within their business, including recommendations for cost-free and cost-effective ways of further improving it. During these initial discussions, I formed good relationships with these three people, built on trust. Each of them soon agreed[27] that their businesses would take part in my research study. Before I discuss in more detail the two stages of the research that I then did within these businesses, I will first outline the documentary analysis stage of my research.

[27] The owner of Business A agreed this at the first meeting. Soon after the first meeting, the IT Manager of Business B and the Chief Executive of Business C sought and gained such agreement from the Board of Directors and the Senior Management Committee, respectively.

### 3.3 Documentary Analysis

The first stage of my research was documentary analysis of government and corporate discourse on cybercrime victimisation and cyber security. Initially, this stage was completed by December 2015, but was then added to as I selected a few more documents for analysis during the months that followed. I did this because those additional documents also contained clear evidence of government thinking in the lead up to its launch of the UK's second National Cyber Security Strategy in November 2016[28]. Ultimately, this documentary analysis stage was completed in September 2016.

It involved the selection and analysis of twenty-five documents, drawn from a period spanning nine years (2007 to 2016)[29]. Most of these were documents produced by the government (18), some were parliamentary (4) and a few were corporate (3). This selection of documents was centred around the UK's first National Cyber Security Strategy (2011-2016), government-led public education/awareness initiatives[30] and government advice to businesses on cyber security, particularly those within the SME sector[31]. It also included a government review[32] and two Parliamentary Select Committee Reports[33] on cybercrime. My selection strategy was based firmly on an intention to gather evidence of all the key government discourse on cybercrime and cyber security within the last decade. But that strategy also sought to access the views of certain other parties, such as academic experts (e.g. in the evidence they gave to Parliamentary Select Committees), and to assess the influence of the commercial sector on government thinking (e.g. cyber insurance companies and cyber security companies working with the government on cyber security initiatives such as *Cyber Essentials*).

Documents such as these can be used to uncover the key discourses and attitudes of policy-makers (and others) about cyber security. In particular, they can demonstrate

---

[28] This second Strategy is set to last until the summer of 2021 (HM Government, 2016b).
[29] A list of all the documents analysed can be found in Appendix F on page 179.
[30] For example, the *Cyber Streetwise* campaign which began in 2014.
[31] For example, the Department for Business, Innovation and Skills's *Cyber Essentials Scheme: Requirements for basic protection from cyber attacks* (DBIS, 2014), *Small businesses: What you need to know about cyber security* (DBIS, 2015), and GCHQ's *Countering the cyber threat to business* – including the *10 Steps to Cyber Security* (GCHQ, 2013).
[32] Home Office (2013) *Cyber Crime: A review of the evidence***.** Home Office Research Report 75. HMSO.
[33] House of Commons Science and Technology Committee (2012) *Malware and cyber crime*. HMSO. House of Commons Home Affairs Committee (2013) *Report on E-Crime*. HMSO.

the direction in which its governance is being steered as part of 'governmentality' (Foucault, 1982) – an approach to government which views certain objectives[34] as being best achieved by acting *through* 'responsibilised' citizens and non-government organisations (Garland, 1997).

### 3.3.1 Framework Analysis

Without strategic planning, this amount of documentary analysis could have been difficult and disordered:

> 'At the first stage of qualitative analysis, the prospect of analysing several hundred pages of transcript can seem quite daunting. It is for this reason that organised steps to 'manage' the data are suggested, in order to make this volume of material easier to access and interpret' (Ritchie *et al.*, 2014, p.297).

To these ends, the method that I employed was 'framework analysis.' This is an approach that uses thematic framework to organise the collected data. The constructed framework comprises a set of descriptive themes that are also subdivided by a succession of related subthemes, all of which have been identified by familiarisation with the original material (Ritchie *et al.*, 2014). Through this process, the data analysis becomes much more refined, and is rendered more transparent (Srivastava and Thomson, 2009; Seale, 2012).

There are five key steps in data management for this type of thematic analysis. Chronologically, these are: familiarising yourself with the data, constructing an initial thematic framework, indexing and sorting, reviewing data extracts, and data summary and display (Ritchie *et al.*, 2014). Use of this framework method enabled me to:

- identify a set of core and subsidiary themes within the 25 selected documents,
- construct thematic matrices,
- observe any relationships and commonalities between the themes and subthemes, and
- produce a descriptive, analytical account based on those observations.

[34] Such as here, the reduction of cybercrime and the promotion of a culture of security consciousness.

From this, it can be seen that the main benefits of this matrix-based format are that it allows the person who is analysing the data to move back and forth between different levels of abstraction without losing sight of the raw data, and facilitates both cross-case and within-case analysis (Ritchie *et al.*, 2014).

I identified two main themes and four subthemes, from which I constructed the matrices. Also, for more specific categorisation within those matrices, I used eleven thematic headings. Those themes, subthemes, headings and the framework matrices themselves can be found in Appendix E on page 175. Once completed, two main pervasive themes emerged from all of this documentary analysis. They were **the responsibilisation of organisations and individuals for cyber security**, and **the shaping of victim status within and around it**. These themes will be discussed in detail within the next chapter.

### 3.4 Observation

I used the method of observation to a small, preliminary extent. Specifically, to gain some knowledge of the physical, social and technological layout of the research participants' office working environments. I made these observations during visits to each of the three businesses, a few days before the start of the Diary Study stages within them. In Businesses A and C, I was given permission to take photographs of the office layouts. However, in Business B this was not possible, it being a busy law firm in which 47 staff were working at the time. Instead, the IT Manager provided me with an excel spreadsheet containing a staff seating plan for each of the three storeys of the office building. All of these data were particularly useful for giving me insight of the social spacing within those working environments.

### 3.5 Diary Study

During July and September of 2015, I conducted the Diary Study stage of my research within these three businesses. First, in Business A (6th-10th July), then in Business C (7th – 11th September), and finally in Business B (14th – 18th September). Doing it in this order worked well because each successive study involved a greater number of participants (3 in Business A, 8 in Business C and 18 in Business B). It is worth noting that these numbers are much less different when viewed in terms of the *proportion* of employees within each business who took part. Specifically, in both Business B and Business C, 38% of their employees participated in the research (18 out of 47

employees and 8 out of 21 employees, respectively). This was a healthy proportion of employee participation, and those participants worked in different departments and at differing levels within those businesses (as requested in my recruitment drive).

It was a five-day Diary Study, conducted online using the *iSurvey* platform, which is a survey-generation and research tool for distributing online questionnaires. This platform was designed/developed at, and is operated by, the University of Southampton.

There were several reasons why I chose to use the Diary Study method in my research. The first was that it met the practical consideration that I could not observe each of the participants individually and constantly for five days within (and beyond) their office working environments. Also, diaries are 'very flexible ways of accessing information about activities and thoughts and feelings' (Alaszewski, 2006, p.112). They capture life as it is lived (Wheeler and Reis, 1991; Sheble and Wildemuth, 2009), and 'provide a record of an ever-changing present' (Allport, 1942). As well as recording events, Diaries can also 'increase the visibility and significance of routine or everyday processes which might be regarded as mundane aspects of everyday life' (Kenten, 2010, p.3). My choice of this method was influenced also by the fact that Diary Studies had been used effectively within Cyber/Information Security research before; specifically, within research on Usable Security (Inglesant and Sasse, 2010; Steves *et al*., 2014).

Diary research is most effective when the design and the research questions are complementary in form (Bolger *et al.*, 2003, p.588). Given that I wanted to investigate people's experiences, attitudes, habits and practices concerning cyber security at work, at 'home', and across/between those two converging contexts, Diary Study seemed a fitting method for achieving this. More specifically, Diaries 'offer the opportunity to investigate social, psychological, and physiological processes, within everyday situations. Simultaneously, they recognise the importance of the contexts in which these processes unfold' (Bolger *et al.*, 2003, p.580). I considered that those attributes would serve my research goals well.

There were other reasons as well for choosing this method. One of the greatest strengths of the Diary Study method is its ability to identify temporal dynamics (e.g. day versus evening). It can also:

> 'help determine the antecedents, correlates and consequences of daily experiences…[and] be used to evaluate whether individuals differ in these processes, and if so, determine the sources of these individual differences' (Bolger *et al.*, 2003, pp.586-587).

Lastly, Diaries are very effective when the phenomena you are studying would not otherwise be accessible because they are internal (i.e. inner thoughts), situationally inaccessible (e.g. cyber security practices at 'home') or because the physical presence of the researcher would significantly impact upon those phenomena[35] (Elliott, 1997; Wheeler and Reis, 1991; Bolger *et al.*, 2003; Sheble and Wildemuth, 2009).

I chose to use the *iSurvey* platform because there a numerous advantages to conducting Diary Study online. Through this medium, data entry, management and accuracy are improved (Iida *et al.*, 2012), and the electronic data collection provides time and date-stamping which, together with carefully designed questions, prevents problems of forgetfulness and uncertain compliance, and also provides a direct measure of compliance (Bolger *et al.*, 2003). Also, conducting it online minimised the risk of skipped questions (Ibid), because on each day the set of questions were presented in sequence, ending only when the whole entry had been completed. To deliver to them the promised anonymity – and thereby meet any security and privacy concerns (Impett *et al.*, 2008; Sheble and Wildemuth, 2009; Iida *et al.*, 2012) – I gave each participant an ID number to use during diary entry. The electronic setting also facilitated prompting, reminding and other communications between me and the participants.

I was also conscious of the dangers that can lie within use of the Diary Study method. The 'Hawthorne Effect' is often mentioned as a possible explanation for positive results in intervention studies. Nowadays, the term is mostly used to refer to 'the behaviour-modifying effects of being the subject of social investigation, regardless of the context of the investigation' (Wickstrom and Bendix, 2000, p.363). Within the literature on Diary Methods, the equivalent term used is 'Reactance.' Therein, it is defined as 'a change in participants' experience or behaviour as a result of participation in the study' (Bolger *et al*., 2003, p.592). However, there seems to be

[35] For example, the observation process changing the atmosphere/feelings/behaviour within the work setting.

little evidence that reactance poses a threat to the validity of diaries. For example, Litt *et al.* (1998) reported that although their participants noted being more aware of monitored behaviour, the behaviour itself was not reactive. In several diary studies, Gleason *et al.* (2001) have documented negative mood elevation in the initial days. In each, the initial spike in negative effect was short-lived, and it dissipated within two to three days. It seems that 'diaries may lead to less reactivity than other forms of data collection because of a habituation process' (Bolger *et al*., 2003, p.592). Indeed, there is some evidence that measurement reactivity associated with self-monitoring may not be a significant problem (Vuchinich *et al*., 1988), and that such effects may be minimal when more than one behaviour is recorded and when participants have no opportunity to review their daily recordings (Hayes and Cavior, 1980). This is another argument for using online diaries, which conceal prior responses from view.

Another danger is that recruitment, retention and the quality of data collected can all be inhibited by potential participants assuming that the process of Diary Study will be time-consuming (Sheble and Wildemuth, 2009). However, these perils can be guarded against through effective pre-test training and careful design of the diary entry protocol (Reis and Gable, 2000; Iida *et al.*, 2012). In each of the three businesses, I held a pre-Study training session, during which I showed the participants the *iSurvey* platform and explained how they would use it, and answered any further questions that they had about either of the two stages of research in which they would take part. Beforehand, I had also emailed each of them a *Participant Information Sheet*[36] which gave them detailed information/instruction on those two stages, and how they would participate in them. At the end of those pre-Study training sessions, I gave each of the participants a hard copy of the *Participant Information Sheet*, asked them to read it again, and then to fill out and sign a *Consent Form*[37] to formally confirm their willingness to participate in the study.

My design of the Diary Study was done very much in recognition of the fact there needs to be a trade-off between the quantity of data sought and the burden placed upon the diarists (Unsworth and Clegg, 2004). Indeed, it is known that 'in order to obtain reliable and valid data, diary studies must achieve a level of participant commitment and dedication rarely required in other types of research studies' (Bolger

[36] A copy of which can be found in Appendix K on page 242.
[37] A copy of which can be found in Appendix L on page 244.

*et al.*, 2003, p.592). Originally, I had planned to conduct the Diary Study over a 7-day period. However, during the recruitment process I realised that it would be prudent to reduce this to 5 days. This definitely aided recruitment, without affecting significantly the prospects of capturing the types and volume of data that I was seeking.

Another possible problem with using the Diary Study method is that, given the potentially heavy burden of commitment that it can place upon participants, researchers can be tempted to design diary instruments that are rather short. In turn, this can limit the depth of reporting that a Diary Study will deliver (Bolger *et al.*, 2003). Again here, I needed to strike a balance. I was careful in my design of the Diary Study as a whole, and the mixture of set and bespoke questions that featured within it during the five days that it ran. In the end, I found that the amount of diary reporting I had asked the participants to do each day was not too burdensome for any of them, and it provided me with a wealth of rich data on the matters that I was investigating.

On each of the five days of the Diary Study, the participants were asked no more than 10 questions (copies of all 47 questions can be found in Appendix M on page 242). This meant that they would spend only about fifteen minutes per day on diary entry, keeping my promise to them[38] that participation in the Diary Study would not take up too much of their time. Use of the online platform also gave them flexibility around *when* they would do this each day or night (and during one or more visits). Each day at about 4pm, I would send a group email to all of the participants containing a link to the next day's Diary Study questions. Here is a copy of one such email:

> Hello Everyone,
>
> Here is a link to the Day 4 Questions https://www.isurvey.soton.ac.uk/17409
>
> Please do not discuss the questions, or your answers to them, with any of your colleagues. This will help to preserve the originality and the accuracy of the data collected during the whole of this study (i.e. both the Diary Study and the follow-up Interviewing). Thanks a lot.
>
> Regards,
>
> Neil.

[38] During the initial recruitment drive, then in the *Participant Information Sheet* (see again note 37), and also in the pre-Study training sessions.

There was a 100% completion rate of these Diary Studies. Across all three businesses, each of the 29 participants answered all of the questions on each of the five days. Another known limitation of the Diary Study method limitation is the potential for participants to may forget to complete the diary, bringing the danger of omitted details during retrospective recording, or even the risk that they might withdraw from the study (Stone *et* al., 1991; Unsworth and Clegg, 2004). However, on only a few occasions did I need to remind/prompt some people to complete their daily diary entry; this they then did no longer than a day later (I kept the links open to facilitate late entry).

### 3.6 Interviewing

As a research method, Interviewing has its critics. For example, Silverman considers it to be a 'romantic impulse in contemporary social science,' elevating the 'experiential as the authentic' (Silverman, 2011, p.179). However, it has been argued that '[such] critiques of interviewing overstate the risks and underplay the potential benefits of robust qualitative interviewing' (Ritchie *et al.*, 2014, p.182), and that interviewing remains 'a core, and effective, method of qualitative data collection' (Ibid., p.55). I certainly found it to be so.

There were several reasons why I chose to use semi-structured interviewing. Firstly, it opens up the interview method 'to an understanding of how interviewees generate and deploy meaning in social life' (May, 2011, p.135). It also embraces the idea that interviewees 'may be making sense of the social world in ways we had not thought of,' and accepts the logic that 'we should be receptive to what interviewees say, and to *their* ways of understanding' (Mason, 2002, p.231). Although this type of interview allows people to answer more on their own terms, it is seen to provide greater structure for comparability than a fully-structured or unstructured interview would (May, 2011), and is thought to be particularly useful when, as I did, a researcher has a specific focus for their interviews within a range of other methods employed in their study (Ibid). Nevertheless, it has been recognised that certain limitations may come from the fact that interviews rely on people's own account of their actions (May, 2011, p.158). Firstly, that their accounts may simply be inaccurate for one reason or another; and secondly, because, while their accounts may be a genuine reflection of

their experiences, there might be circumstances or events surrounding these of which they were unaware (Ibid). However, arguably the only way to achieve the fullest understanding of such things is by witnessing those very contexts and events oneself. Yet I could not have done this in my chosen research: neither extensive observation of (all) participants during their working days in these busy organisations, nor observation of them beyond their work offices (e.g. at home in the evenings), would have possible.

More specifically, I chose the 'Diary Interview' technique. An interview is a 'conversation with a purpose' (Webb and Webb, 1932, p.130). The specific purpose of the 'Diary Interview' is to ask detailed questions about the diary entries, in pursuit of a greater depth of understanding (Kenten, 2010). It is considered to be one of the most reliable methods of obtaining information (Corti, 1993). It also enables further exploration of the context in which the entries were made, which then assists in the analysis of the diary content, and reduces the risk of analytical misinterpretation (Kenten, 2010). As well as giving opportunities for elaboration on their diary entries, the interviewing would provide a counterpoint to the participants' diaries, enabling me to do several things: Firstly, to identify and explore any anomalies and inconsistencies identified during diary entry analysis. Secondly, to question each participant about their understanding and interpretation of their employer's cyber security policy, and their level of compliance with it (and the reasons behind any incidents/practices of non-compliance). And thirdly, to gain further insight of the responsibilisation processes within the three companies, and pick up on any participant fears of blame and sanction for cyber security policy breaches. Beyond individuality, the whole interviewing process would also alert me to any collective behavioural and attitudinal trends.

My choice of the 'Diary Interview' technique required a temporal balance to be struck: I needed to read and reflect upon all of the participants' diary entries before interviewing them, but I also wanted those interviews to take place relatively soon after their completion of the Diary Study stage. In practice, within all three businesses, I conducted the Interviewing stage about a month after the finish of the

Diary Study stage[39]. While in total 29 people had taken part in the Diary Study stage, there were only 28 participants in the Interviewing stage. This occurred because in Business A, during the time between those two stages, one of the participants (P3/A) was dismissed by their employer (P1/A) for two alleged breaches of cyber security[40].

All of the interviews were conducted on a one-to-one basis. On average, each interview lasted 40 minutes[41]. In each of the three businesses, I conducted all of the interviews within a private room that had been provided for that purpose. On each of these occasions, myself and the interviewee were the only people present in the room during the interview. Before starting their interview, to each interviewee I said:

- Thank you for completing the Diary Study, and for sparing the time to be interviewed.
- That if they found that they did not want to answer any (or all) of the questions put to them during the interview, they were under no obligation to do so.
- That at any time, and for any reason, they could if they wished ask for the interview to cease.
- That, with their consent, I would audio-record their interview (to facilitate the transcription of the interview data into written form later on)[42].
- That there was a glass of water already provided for them, should they want a drink during the interview.
- That if at any time during the interview they wanted a pause, not to hesitate to ask for one.

There was a 100% completion rate during this Interviewing stage. All 28 of the participants attended an interview, and answered all of the questions that I put to them.

[39] Business A (12th August 2015), Business C (5th, 6th and 7th October 2015) and Business B (12th, 13th, 21st and 28th October 2015).
[40] Details of these alleged breaches are given later on, in note 77 on page 78.
[41] However, the average interview time was different within each business: Business A (53 minutes), Business B (29 minutes) and Business C (39 minutes).
[42] All 28 interviewees gave their consent to such recording.

### 3.7 Transcription of the data from the Diary Study and Interviewing stages

When each Diary Study was completed within a business, I downloaded the data from *iSurvey* (in excel spreadsheet form) to read it and reflect upon it before interviewing those diarists. Eventually, after completion of both the Diary Study and Interviewing stages in all three business, I placed all of the Diary entry data into five excel spreadsheets. This made it easier for me to look at the diary entries of all 29 participants on any of the 5 study days.

When all of the interviews had been conducted in all of the businesses, I transcribed the audio-recorded data from them into written form (in Word documents). This took several weeks, but was made easier by my use of transcription software (along with headphones and a transcription pedal). Also, through this process of transcription I became very familiar with all of that data.

### 3.8 Analysis of the data from the Diary Study and Interviewing stages

Again, the method that I employed in my scrutiny of this data was framework analysis. Through it, I identified three main themes and ten subthemes, from which I constructed the matrices. Also, for more specific categorisation within those matrices, I used eighteen thematic headings. Those themes, subthemes, headings and the framework matrices themselves can be found in Appendix H on page 205.

# Chapter 4: Documentary Analysis

## 4.1 Introduction

Successive governments have warned of the growing dangers that cyberspace can bring to the UK and its citizens, setting this clearly within the wider context of national security. Before looking closely at such government discourse on cybercrime and cyber security, it is important to mention recent calls for change in governments' overall strategy towards national security. Specifically, for a new approach to it, 'designed from the outset to respond to the major risks as they may affect the citizen, rather than the institutions of the state' (Omand, 2010, p.309). It has been argued that there need to be certain shifts in government thinking on this matter: Firstly, a shift to an all-risks approach, based on the principles of risk management. Secondly, a shift towards governmental *anticipation* of the risks. And lastly, a shift towards 'the promotion of a more resilient society, placing new demands on government to work with communities and with industry and commerce' (Ibid).

In 2011, when delivering the UK's first Cyber Security Strategy, the coalition government observed that:

> 'As with most change, increasing our reliance on cyberspace brings new opportunities, but also new threats. While cyberspace fosters open markets and open societies, this very openness can also make us vulnerable to those who want to harm us by compromising or damaging our critical data systems' (Cabinet Office, 2011, p.7).

Similar warnings continue to be given. For example, in November 2015 the then Chancellor of the Exchequer reiterated that 'the internet represents a critical axis of potential vulnerability for this country and its people' (HM Treasury, 2015, p.4)[43]. In this way, the government describes cyberspace as a place of great business opportunity, but in which great risk also lies.

[43] These comments were part of a speech given by George Osborne MP at GCHQ, in which he laid out plans to more than double government spending on cyber security (to £1.9 billion) as part of a 'National Cyber Plan.' The speech at GCHQ formed part of the government's Spending Review and Autumn Statement of 2015.

To control the dangers of that risky environment, the government has been placing upon non-governmental actors an increasing responsibility to protect themselves and others. This message has been directed both at non-governmental organisations (NGOs) and individual citizens. Over time, the reiteration of that responsibilisation narrative has grown stronger, through more frequent delivery and by using language of increasing urgency. The State continues to push responsibility away from itself and onto non-State actors as a means of both extending and enhancing the governance of situations and environments which have a tendency to produce criminal behaviour[44] (Garland, 1997).

However, that responsibilisation strategy itself brings dangers. Blame features within any form of risk management (Sparks, 2001; Garland, 2001). In this one, the problem of victim blaming lurks. This is the practice of holding the victim of a crime *unduly* responsible (wholly or partially) for the harm that has befallen them. Indeed, responsibilisation and victim blaming can be seen as two sides of the same coin. Almost invariably, responsibilised actors will be denied the status of *legitimate* victim unless they are deemed to have been *blameless* (Christie, 1986). Gaining legitimate victim status is important because it can attract support (personal, social, financial, commercial, legal), whereas failure to gain it can attract criticism and liability (personal, social, financial, commercial, legal). In this way, where victims do not meet that ideal standard they will suffer blame, and the consequences which can flow from it. However, legitimate victim status can be truly elusive, almost impossible to attain. This is particularly so within cyber security, because in many cases some (in)action on the part of the victim can be identified to show that they were not completely blameless in their plight. This also reveals another danger brought by responsibilisation, which is that the focus of blame can sometimes shift unduly from the true offender to the hapless victim.

During my reading of many documents concerned with government and commercial discourse on cyber security and cybercrime victimisation, I was able to identify two main themes that pervaded them. These were **the responsibilisation of organisations and individuals for cyber security**, and **the shaping of victim status within and**

[44] Known also as 'criminogenic situations.'

**around it**. I also identified a range of accompanying subthemes[45]. In this chapter, I will report and comment upon those themes and subthemes, thereby highlighting the ways in which responsibility is being placed upon small businesses for their own cyber security, and that of others with whom they trade and communicate. Although the majority of this chapter will be focused on political rhetoric and discourse, it will also include discussion of some non-government and near-government organisations that are involved in reproducing and reinforcing those governmental narratives, such as banks and the police.

## 4.2 Corporate and individual responsibility for cyber security

A key theme identified within these documents was that *we all benefit from cyberspace, so we all have a responsibility to protect it*. In 2011, the government declared that 'with the rise of cybercrime, what was a concern primarily for the defence and intelligence elements of government is now something that concerns all of us' (Cabinet Office, 2011, p.25). Recognising that the achievement of its cyber security vision for the UK in 2015 would 'require everybody, the private sector, individuals and government to work together' (Cabinet Office, 2011, p.22), it considered that:

> 'the debate [on developing norms of acceptable behaviour in cyberspace] must involve all those with a stake in an open, trusted and stable cyberspace, including industry, business and representatives of civil society' (Ibid, p.27).

Since then, GCHQ has also made clear its view that 'cyber security is not just an issue for governments – it's for companies and citizens too' (GCHQ, 2013, p.8).

### 4.2.1 The responsibilisation of organisations

UK business continues its firm embrace of web and internet technologies, and the UK population 'is the world's most advanced adopter of online retail and the digital economy' (Department of Business, Innovation and Skills (DBIS), 2015c, p.5). Yet, security concerns have accompanied this growth, heightened also by a spate of hacking attacks on companies, such as that upon *Talk Talk* in October 2015 (which I

[45] See Appendix F on page 179 for a list of those documents. See also Appendix E on page 178 for a listing of the thematic framework used during that Documentary Analysis. See also Appendix G on page 183 for the data drawn from those documents set within that thematic framework.

will discuss in some detail within section 4.2.2). Amid such concerns, as part of its continuing strategy of responsibilisation, the government has kept trying to enlist non-State actors in the governance of this criminogenic situation, particularly businesses within the private sector.

In my analysis, I found that the strongest responsibilising message from government to businesses has been that *businesses have a responsibility to protect themselves, and by so doing, protect others*. Government advice on how businesses should do this has become increasingly vehement. In October 2014, it stated unequivocally that:

> '[R]egardless of their size, use of technology, the industry sector in which they operate and their global presence, every organization needs to implement a robust and effective approach to cyber security' (DBIS, 2014, p.13).

In this way, the government has been requiring businesses to adopt the philosophy of 'target hardening' (Clarke, 1983). Along with enhanced individualism and responsibilisation, target hardening has been one of the ways in which Neoliberalism has shaped the concept of Risk (O'Malley, 2006) in its search for solutions to the 'crime problem' (Karmen, 1990; Walklate, 1997). More specifically, target hardening has been part of Situational Crime Prevention. It emphasises proactive, preventative action against crime by non-State actors, including commercial firms (Garland, 2001).

Businesses have been told to change their collective mindset on cyber security. In March 2015, while announcing joint initiatives between itself and the cyber insurance sector, the government emphasized the need for businesses 'to move away from treating cyber primarily as a technology or security issue, to one that is owned collectively as a key risk to firm viability and that permeates the way the business is run' (Cabinet Office, 2015a, p.5). It also cited 'a clear conclusion…that some businesses still feel that they do not fully understand the risk of cyber attack properly,' claiming that 'this highlights the need for companies to have clear accountability structures for cyber risk, and to put in place robust cyber security risk management arrangements' (Cabinet Office, 2015a, p.1).

The government has given businesses more specific advice on this, and how they can harden themselves as targets. For example, it has advised small businesses to put in place a number of cyber security measures, within a three-pronged approach (DBIS, 2015): First, *get the basics right*, which include downloading software updates in a

timely fashion, using strong passwords, using anti-virus software, and training your staff about cyber security threats and how to deal with them (DBIS, 2015, p.5). Second, *take a risk management approach*, which involves understanding the risks that cyber insecurity could bring to your business[46] (DBIS, 2015, p.6). And lastly, *gain Cyber Essentials accreditation*, which in turn enables businesses 'to advertise the fact that [they] adhere to a government-endorsed scheme' (DBIS, 2015, p.12).

The fact that organisations are now viewed simultaneously as potential victims *and* unwitting accomplices to cybercrime simply toughens the responsibilisation rhetoric towards them. Indeed, the main reason for the government's sharper focus on SMEs is that cybercriminals 'often attack a company's supply chain as a way of outflanking its security' (Symantec, 2015), and there has been a growing trend of cybercriminals targeting employees in SMEs, in order to achieve onward malware infection of larger companies with which they do business (MacEwan, 2013). It has been observed that:

> '[T]hese organisations often have fewer resources to invest in security, and many are still not adopting basic best practices…[which] puts not only the businesses, but also their business partners, at higher risk' (Symantec, 2015, p.6).

The government recognises this additional risk, and has sought to make businesses aware of it when advising them on cyber security. Specifically, for example, by listing 'damage to other companies that you supply or are connected to' as one of the serious potential impacts of a cyber attack (DBIS, 2015, p.6). Indeed, the supply chain has been described as 'the elephant in the room when we talk about cyber security' (Whitehouse, 2016), and the government continues to call upon businesses to protect, not only themselves, but other organisations with which they have links.

Leading by example, the government has strengthened its own supply chain. Since October 2014, it has required all organisations that bid for certain types of governmental contracts[47] to be *Cyber Essentials* accredited, and to be reassessed

[46] More specifically, this *risk management approach* involves the business asking itself the following questions: What is directly at risk? Who could pose a threat to these assets? What form could the threat take? What impact could an attack have? And how bad could it be*?* (DBIS, 2015, p.6).
[47] Specifically, those contracts 'which feature characteristics involving the handling of personal information and the provision of certain ICT products and services' (Cabinet Office, 2016b, p.1). Originally, the Ministry of Defence was excluded from the procurement policy, but from 25th May 2016

annually[48]. Designed to be 'light touch' and achievable at low cost (Cabinet Office, 2016b), the *Cyber Essentials* accreditation scheme was created to fulfil two functions: First, to provide 'a clear statement of the basic controls that all organisations should implement to mitigate the risk from common internet-based threats.' And second, '[to] offer a mechanism for organisations to demonstrate to customers, investors, insurers and others that they have taken these essential precautions' (DBIS, 2014b, p.3). The government considers that the *Cyber Essentials* scheme 'defines the minimum set of security controls that an organisation should have in place' (Cabinet Office, 2015c, para. 4.1). However, there is also an enhanced form of the scheme (*Cyber Essential Plus*), and all of this is set within the context of further governmental instruction to organisations on how they should be improving their cyber security (e.g. *10 Steps to Cyber Security*[49]). These 'gatekeeping' guidelines and protocols can be seen as a technique of government-at-a-distance (Garland, 1997), through which the State responsibilises non-State actors and prompts them to act in crime-controlling ways (O'Malley, 1992; Garland, 1996).

Here, it is important to mention the role that cyber security companies continue to play in the framing of such campaigns and initiatives. One criticism has been that:

> '[T]he advice [that features in them] usually comes from security experts and service providers, who monotonically repeat suggestions such as 'use strong passwords' (Bada and Sasse, 2014, p.33).

Alone, such advice cannot 'fix' cyber security problems; it must be given in conjunction with other influencing strategies in the shaping of an organisation's cyber security culture (Ibid). There is also a risk that commercial interest may influence the framing of any advice given to, and other cooperation with, the government: cyber security companies have a growing number of products and services to sell. Furthermore, beyond design, many cyber security companies are actually involved in the *delivery* of some schemes, such as *Cyber Essentials* and *Cyber Essentials Plus*, increasing further their (commercial) interest, and potential influence, in these matters.

---

*Cyber Essentials* accreditation has also been required of all contractors and suppliers entering into new contracts with the defence forces (Cabinet Office, 2016b, p.1)

[48] Cabinet Office, 2016b, p.9.

[49] National Cyber Security Centre (2017) *10 Steps to Cyber Security*. See further at https://www.ncsc.gov.uk/guidance/10-steps-cyber-security

Increasingly, insurance companies also feature in this fray. As part of its recent push 'to use insurance as a driver for improving cyber security practice in UK businesses, and SMEs in particular' (Cabinet Office, 2015a, p.2), the government has taken the further step of linking *Cyber Essentials* accreditation to cyber insurance products. More specifically:

> '[A]s an encouragement to adopt the scheme, insurers will now look to include *Cyber Essentials* certification as part of their small and medium-sized enterprise (SME) cyber risk assessment….[and there will be] a type of cyber insurance cover for SMEs that pays for the cost of *Cyber Essentials* certification to reflect the risk reduction that accreditation represents' (Cabinet Office, 2015, p.5).

Insurance itself can be seen as a technology of governance, promoting a form of 'responsibilised autonomy' in which the insured must pay regular premiums and stay within specified behavioural limits (Garland, 2001, p.181). In June 2015, the government reported 'a notable drop' in the percentage of organisations who claim to have cyber liability insurance cover, either under general insurance policies or specific cyber insurance policies (DBIS, 2015a, p.28). As evidence of this, it presented survey results which revealed that only one third of businesses believe they have insurance that would cover them in the event of an information security breach (Ibid). Indeed, earlier that year the government had urged businesses 'to value the risk of cyber attack properly,' reporting that 'many [of them] are overestimating the extent to which their insurance provides cover for cyber risk' (Cabinet Office, 2015a, p.1).

### 4.2.2 Heightening the rhetoric of responsibilisation

My analysis has identified a change in tone within more recent government discourse. The responsibilisation rhetoric has been ramped up. This has resulted from the government's growing frustration with what it sees as corporate irresponsibility around cyber security. One of the specific causes of this frustration has been increased attacks on high-profile companies within the retail sector, and the wealth of customer data which they hold. In April 2015, within its annual Internet Security Threat Report, Symantec observed that:

> 'Attackers clearly have retailers in their cross hairs, if the increase in data breaches containing financial information is any indication…[and] the

> prevalence of data breaches over the past number of years has certainly had an impact on consumers' views concerning their private information' (Symantec, 2015, pp.83 and 84).

Six months later, the *Talk Talk* hack soon provided the UK's most publicised example of this. As the facts of that incident emerged, it became clear that *Talk Talk* had 'failed to take adequate steps' to protect its customers' data (Information Commissioner's Office, 2016), by not implementing 'the most basic cyber security measures' (Information Commissioner, quoted in BBC, 2016a). The direct costs of the attack to the company amounted to £42 million. It also lost more than 100,000 of its customers, and saw its annual profits halve (BBC News, 2016). The personal data of 157,959 *Talk Talk* customers were accessed during the attack, including the bank account numbers and sort codes of 15,656 customers (Information Commissioner's Office, 2016, p.4).

A week after the incident, the House of Commons' Culture, Media and Sport Committee launched an inquiry into it. Within its subsequent Report, it was highly critical of *Talk Talk*'s poor cyber security, including the fact that the attack had exploited one of the oldest and best-known vulnerabilities on the web (SQL injection[50]). The Committee declared that:

> 'It is no longer a defence for a company using an e-commerce platform to say that it was not aware of the risk of SQL injection-based attacks, or…[similar] forms of cyber-penetration' (House of Commons Culture, Media and Sport Committee, 2016, p.7).

Beyond the criticism of *Talk Talk* itself, these words reflected that rising frustration around cyber security, and the government used the incident as part of a general warning to businesses in the UK. A month after the attack, the Minister for the Digital Economy called upon organisations to view it 'as a timely reminder that we need to take action to protect ourselves,' hoping that 'businesses around the country are taking the opportunity to review how they deal with cyber security' (Department of Culture, Media and Sport (DCMS), 2015, pp.1 and 2). He stated firmly that:

[50] SQL injection is a type of security exploit in which the attacker adds Structure Query Language (SQL) code to a web form input box, to gain access to resources or make changes to data.

> '[T]he UK is a world leader in the use of digital technologies, but we also need to be a world leader in cyber security. Trust and confidence in UK online security is crucial for consumers, businesses and investors' (Ibid).

Given that much of cyberspace is owned and used by private companies, the government has kept its view that the private sector can, and must, contribute greatly to securing UK cyberspace. In 2007, the House of Lords Science and Technology Committee stated that 'businesses operating online should take their share of responsibility for reducing risks in [some key] areas,' including the prevention of cybercrime (House of Lords Science and Technology Committee, 2007, p.61). Within its (first) Cyber Security Strategy, the government envisioned a crucial role for the private sector (Cabinet Office, 2011, pp. 23 and 32), and it continues to make reference to 'an ongoing partnership [between government and industry] to address cyber threats to UK businesses and to wider UK interests' (Cabinet Office, 2015, p.2).

However, very few organisations have gained accreditation under the *Cyber Essentials* scheme[51]. This is despite the government's continuing claim that businesses could prevent the vast majority of cyber attacks on themselves if they put in place the simple security controls advocated within the *Cyber Essentials* scheme (DCMS, 2015a, p.3; DBIS, 2015d, note 2; DCMS, 2016, p.2). Indeed, in 2015 the Head of CERT-UK (the National Computer Emergency Response Team) stated: 'If *Cyber Essentials* accreditation was widespread, 80% of my work would disappear'[52].

Again here, the tone of governmental comment has been sharpening. For example, when introducing the results of the government's 2015 Information Security Breaches Survey, the Minister for the Digital Economy stated that 'all businesses and organisations should adopt the *Cyber Essentials* scheme as a vital first step – no ifs or

[51] On 21st July 2016, I sent a Freedom of Information (FOI) request to the Department for Business, Energy and Industrial Strategy, asking for up-to-date numbers of *Cyber Essentials* and *Cyber Essential Plus* certifications. On 10th August, they replied that they did not have those numbers, and directed me towards the Department for Culture, Media & Sport. I then sent a FOI request to that Department. They replied that they did not have these numbers, and referred me to the Cabinet Office. I then sent a FOI request to that Office. They replied that they did not have these numbers, and referred me back to the Department for Business, Energy and Industrial Strategy. Note, however, that in September 2015 Intel Security UK claimed to be 'the 1000th company to achieve Cyber Essentials certification status' (DMCS, 2015, p.2), and that in December 2016 it was declared that 2,673 certificates had been issued since November 2015 (HM Government, 2016d, p.15). So, adding those two figures together, it can be estimated that by December 2016 fewer than 4000 companies had gained accreditation under this scheme. Note also, that there are 5.5 million private sector businesses in the UK, 99.9% of which are SMEs (Federation of Small Businesses, 2016).

[52] Chris Gibson, Director, CERT-UK, *Cyber Security Summit*, London, 18 November 2015.

buts' (DBIS, 2015a, p.4); and more recently, his ministerial successor expressed again this governmental view 'that every organisation which relies on the internet for business should have *Cyber Essentials* as a minimum' (DCMS, 2016, p.2).

The government's frustrations seem more predictable when viewed again in the wider context of 'governmentality' (Foucault, 1978). Power is no longer a matter of the State imposing its will (Rose and Miller, 1992; Garland, 1997). Rather than 'owning' power, governments now enlist the cooperation of others, whose actions then 'translate' power in order to realise governmental objectives (Rose and Miller, 1992; Garland, 1997). Within this government-from-a-distance (Osborne and Gaebler, 1992; Latour, 1987), that enlistment/enrollment process:

> 'always entails activity on the part of the 'subjects of power,' and therefore has built into it the probability that outcomes will be shaped by the resistance or private objectives of those 'acting down the line'' (Garland, 1997, p.182).

Here, the woeful uptake of the *Cyber Essentials* scheme by businesses suggests that such resistance and/or competing tensions, or some other factors, are at play.

So, there is evidence that advice and encouragement given directly by government to businesses has lacked efficacy. There is also evidence that the government has enrolled some other actors in this task of responsibilisation, but that their efforts have been failing as well. For example, originally the government consulted the Federation of Small Businesses (FSB) in the design of the *Cyber Essentials* scheme (Cabinet Office, 2016b, p.3), and subsequently the FSB has tried hard to convince its members to participate in it. Reminding them that 'the government is looking towards small businesses for economic growth and to create jobs' (FSB, 2013, p.8), the FSB has stated that 'alongside the action that government and the public sector need to take [regarding cyber security and cybercrime], businesses need to help themselves more' (FSB, 2013, p.4). However, the inertia around *Cyber Essentials* may have contributed to a stronger tone in some of its later statements, such as the one stating that 'too many firms ignore the threat of cybercrime' (FSB, 2015). Recently also, the Institute of Directors (IoD)[53] has been similarly critical of its members, declaring that 'businesses are not taking cyber security seriously enough' (IoD, 2016, p.1).

[53] Around 70% of the Institute of Directors' 34,500 members come from SMEs (from all industries), and are typically in senior management and boardroom level positions.

The government considers that, along with *Cyber Essentials* accreditation, all businesses should have cyber insurance cover as part of their risk management strategy. However, its own evidence suggests that, thus far, many of them are not responding to these calls. Certainly, businesses have been reluctant to purchase cyber insurance because of the cost, and too many exclusions, restrictions and uninsurable risks (Experian, 2013; Alloway and Kurcher, 2014). Also, the government itself has recognised that 'in a nascent market, the terms and coverage of policies vary tremendously' (DBIS, 2015a, p.29). However, as that market matures, the pressure for businesses to take up such insurance will intensify. Also, new laws may yet bring change. In June 2015, the government reported that:

> '[T]he impending revision of the EU Data Protection Regulation regime is expected to include mandatory notification of breaches of personal data, and this may well be the catalyst to change the cyber liability insurance landscape in the UK' (DBIS, 2015a, pp.28-29)[54].

Now, the UK is leaving the European Union (EU). However, Brexit will probably not change this particular issue because, soon after the EU referendum result, the government stated that 'if the UK remains within the single market, EU rules on data [protection] might continue to apply fully in the UK, [and] in other scenarios we will need to replace all EU rules with national ones' (DCMS, 2016a, p.1). The latter will likely occur, and the UK government has recently made clear its intention to pass legislation that mirrors the key provisions of the EU's General Data Protection Regulation (GDPR) and its Network and Information Security Directive (NIS) as well[55]. In any case, as the process of Brexit continues, UK government discourse continues to demand urgently that organisations join the *Cyber Essentials* scheme and purchase cyber insurance, while citing competitive advantage as an extra benefit that will flow from this. Indeed, the government continues to tell businesses that gaining *Cyber Essentials* accreditation:

[54] The EU's General Data Protection Regulation will apply from 25th May 2018 onwards.

[55] The NIS Directive imposes on certain organisations new obligations to report cyber security incidents to regulators and affected customers. The organisations taking on these duties will be those deemed to be 'essential services,' within market sectors considered central to the operation of the economy, etc. These include Finance, Utilities, Healthcare and Digital Services. The NIS Directive came into force in August 2016. From then, EU Member States were given 21 months in which to implement it within national law.

> 'will provide independent assurance that you have the protections correctly in place…[and] you will also be able to display the *Cyber Essentials* badge to demonstrate to customers, partners and clients that you take cyber security seriously – boosting reputations and providing a competitive selling point' (HM Government, 2017, *Cyber Aware* website[56]).

All of this places further pressure on businesses – particularly SMEs – to improve their cyber security, including the responsibilisation conundrum of getting *each* of their employees to behave securely, *all* of the time.

### 4.2.3 The responsibilisation of individuals

The message that *humans are the weakest link in the cyber security chain* continues to feature within government discourse (e.g. Cabinet Office, 2016b, p.2). My analysis also revealed that this message has often been accompanied by another, which is *that every person within an organisation has a role to play in keeping it secure*. In the (first) UK Cyber Security Strategy, the government made clear its view that 'ordinary people have an important role to play in keeping cyberspace as a safe place to do business and live our lives' (Cabinet Office, 2011, p.22). Since then, that message has been repeated regularly. For example, within its *10 Steps to Cyber Security*, GCHQ stated that 'all users have a responsibility to manage the risks to ICT and information assets' (GCHQ, 2013, p.10). Soon after, the Department for Business, Innovation and Skills stressed the importance 'that everyone understands their role in keeping the business secure' (DBIS, 2015, p.8). It also reported that:

> '[B]reaches are increasingly due to people within an organisation….[and that] whilst technical controls have their place, organisations should take the opportunity to question the balance between their investment in technical controls and measures to address human factors' (DBIS, 2015a, p.19).

Here again then, the government has been calling for 'target hardening,' and that message has been pitched both at businesses *and* the individuals who work in them. The government views employees, individually and collectively, as a crucial means to that end.

---

[56] Specifically, within the section concerned with the *Cyber Essentials* scheme, on the page entitled 'Protect your own business against cyber threats.' See further at https://www.cyberaware.gov.uk/cyberessentials/

In 2011, part of the government's vision for the UK in 2015 was that its citizens would understand that 'as in the offline world, we are each responsible for our behaviour in cyberspace' (Cabinet 2011, p.23). Since then, it has tried to educate them and change their behaviour through two websites. *Get Safe Online*[57] provides people (and businesses) with a wealth of free information on how to protect themselves, their computers and their mobile devices from many problems online[58]. It is run by a public/private sector partnership that is supported by the government and leading organisations from various sectors, including banking, retail and internet security.

In 2014, the government launched its own website, called *Cyber Streetwise*[59], for the same purposes. A message from the government to individual citizens that emerged from my analysis was that *they need to keep themselves safe by following some basic rules of cyber security*. In 2007, the House of Lords Science and Technology Committee noted wisely that:

> 'There are two key aspects to improving the ability of individuals to manage online security. One is to promote awareness of the risks online, the second is to instill knowledge of how practically to manage them. Both are necessary – one without the other is of little use' (House of Lords Science and Technology Committee, 2007, p.55).

Then, in 2011 the government stated that:

> 'By 2015, we want a UK where people know how to get themselves a basic level of protection against threats online, have access to accurate and up-to-date information on the online threats that they face, and the techniques and practices they can employ to guard against them' (Cabinet Office, 2011, p.22).

The materials made available to individuals (and businesses) through the *Get Safe Online* and *Cyber Streetwise* websites seek to do these things.

Again then, in pursuit of several goals, the government has been urging its citizens to target harden. Through such education, it has sought to reduce the chances of citizens falling victim to cybercrime, thereby also reducing the chances of them

[57] https://www.getsafeonline.org/
[58] E.g. Internet fraud, Identity Theft and malware infection.
[59] https://www.cyberstreetwise.com/ . Note, however, that in October 2016 the name of this campaign was changed to *Cyber Aware* – see now www.cyberaware.gov.uk

passing victimhood on to others (i.e. as unwitting accomplices to onward/ongoing cybercrime). Also, by promoting cyber-secure behaviour in citizens' personal lives, the government has been seeking to deepen and extend the cyber security education that *it hopes* they are receiving in their working lives. However, there is evidence that these education campaigns have been much less impactful than the government thought they would be. For example, in July 2016, when citing recent statistics which reveal that the majority of people in the UK still do not always download the latest software updates for their mobile phones (70%) or their computers (65%) as soon as they are available, the government launched the #quickupdates campaign, to yet again urge people (and businesses) to act in this way (HM Government, 2016a).

Essentially, however, the government continues to delegate to others the task of responsibilising individuals for cyber security. It responsibilises organisations, expecting them in turn to responsibilise their staff. To this end, I found that the government has sent out two main messages to organisations[60]. The first is that *they must inform and train user behaviour*. In January 2014, when launching the *Cyber Streetwise* website, the Home Office declared that 'an educated workforce is the main line of defence against online threats in business' (Home Office, 2014). Increasingly, the government urges organisations to make their staff aware of cyber security threats (DBIS, 2015, p.5), and then maintain their awareness (GCHQ, 2013, p.10). It has kept the view that basic information risk management can prevent most cyber attacks[61], and continues to demand that organisations ensure that their staff 'have appropriate training, so that everyone understands their role in keeping the business secure' (DBIS, 2015, p.8). The other message has been that organisations *must monitor, restrict and discipline user behaviour*. The government expects even small businesses 'to monitor the use of all equipment and IT systems, collect activity logs, and ensure that [they] have the capability to identify any unauthorised or malicious activity' (DBIS, 2015, p.9). It also continues to preach the Least Privilege Principle, under which users are provided only with the access/authority they need to do their job (GCHQ, 2013, p.13). Indeed, the government has declared it best practice to restrict as many permissions as possible (Home Office, 2014), and this includes

[60] Particularly to businesses; and more recently, particularly to SMEs.
[61] This consistent line has run through the following government documents: Cabinet Office, 2011, p.31; House of Commons Science and Technology Committee, 2012, p.19; GCHQ, 2013, p.9; Cabinet Office, 2014, p.7; DCMS, 2015a, p.3; DBIS, 2015, p.4.

keeping third party access to IT equipment, systems and information to the absolute minimum (DBIS, 2015, p.9).

Remote working brings implicit vulnerability, and the government has instructed a lot on this matter. Organisations have been told to choose remote working options which offer an appropriate level of security for their business (Home Office, 2014); and this includes considering whether there is a real need for remote connectivity to their network. If the main purpose is access to files, then businesses should consider moving them into the cloud (Home Office, 2014). Where remote working takes place, the government urges all organisations to restrict the use of removable media, and to ensure that sensitive data is encrypted when stored on devices[62] or transmitted online, so that it can be accessed only by authorised users (DBIS, 2015, p.9; Home Office, 2014). Indeed, the government has warned about complacency in the management of risks presented by mobile devices, reporting that 'one in five small organisations still have not taken any steps with the use of smartphones or tablets, even though the number of breaches through mobile devices has doubled' (DBIS, 2015a, p.30).

This continuing, determined push towards the governance of cyber security by non-governmental organisations has brought with it a multitude of in-house rules. Another subtheme that I identified relates directly to this, and to the core of my research. That message has been that *individuals have a personal responsibility to comply with cyber security policies*. As I have shown, government discourse continues to emphasise that people are the main vulnerability within cyber security (e.g. DBIS, 2015a; Cabinet Office, 2016a). In its 2015 Information Security Breaches Survey, the government reported that the respondent companies:

> 'believe[d] that inadvertent human error (48%), lack of staff awareness (33%) and weaknesses in vetting people (17%) were all contributing factors in causing the single worst breach that organisations suffered' (DBIS, 2015a, p.14).

A year later, the Minister for the Cabinet Office reiterated that 'the tech may have got smarter, but the biggest weakness in any system is still the human being' (Cabinet

[62] E.g. PCs, Laptops, Tablets, Smartphones, USB Drives.

Office, 2016a, p.2). Given this, the government's message to individuals remains unequivocal, and delivered in uncompromising tone: 'Without exception, all users should be aware of….their responsibility to adhere to security policies' (GCHQ, 2013, p.13). Along with this, it continues to demand that organisations 'establish a formal disciplinary process, making staff aware that any abuse of security policy will result in disciplinary action' (GCHQ, 2013, p.14). Respectively, these two strong messages continue to feature within *Steps 4* and *5* of the government's much-promoted *10 Steps to Cyber Security* (Ibid). However, there is also the potential for victim blaming within such processes. For example, given some of the possible repercussions of cyber attack (e.g. legal and commercial), the temptation to blame an attack mainly or solely on the conduct of an employee, and portray that to others[63] as aberrant behaviour aboard a usually tight ship, can be strong.

### 4.3 Victim Status

It has been recognised that 'acquiring the status of victim involves being party to a range of interactions and processes, including identification, labelling and recognition' (Mythen, 2007, p.466). As noted previously (in section 4.1), responsibilisation can complicate the claiming of victim status, and very different consequences may flow from the presence or absence of that status. The *nature* of the responsibilisation itself seems to determine this: the perspective from which it is done (and by whom), its manner, tone and degree. A number of the examples that I have already given as evidence of the government's responsibilisation narrative could also serve as proof that, through its discourse, it has been determining the boundaries of (legitimate) victimhood – in essence, shaping victim status. In this section, I will present further evidence of this.

#### 4.3.1 Victim Precipitation

As others have noted, a corollary of responsibilisation is the ability to delineate 'victimhood' and, through this, either ascribe or deny victim status to those who have suffered harm (Walklate, 1997; Garland, 2001; O'Malley, 2006; Hopkins, 2016). Where an actor (individual or corporate) is seen to have precipitated that harm – which could include failing to prevent it (e.g. *Talk Talk*) – they can lose the ability to

[63] E.g. Regulators, insurance companies, business partners, the media.

identify as a victim (Eigenberg and Garland, 2008). My documentary analysis identified a number of examples of the government framing victim status in this way. Viewed in terms of 'governance' (Rhodes, 1997) and 'governmentality' (Foucault, 1982), they demonstrate how the government has been 'steering' these matters (Osborne and Gaebler, 1992).

One example comes from a speech made by the then Chancellor of the Exchequer in November 2015, in which he emphasized that 'companies need to protect their own networks, and harden themselves against cyber attack'[64] (HM Treasury, 2015, p.4). With words such as these, the government has been putting further pressure on the 5.5 million private sector businesses in the UK – 99.9% of which are SMEs (Federation of Small Businesses, 2016) – to spend more time, money and resources on protecting themselves, and others, from cybercrime. The former Chancellor was speaking only a month after the *Talk Talk* hack, which epitomised what he was referring to. Evidence of *Talk Talk*'s poor attention to cyber security led to it being labelled as much a precipitant as a victim of the attack. Following investigation of this incident, it received the largest fine ever imposed by the Information Commissioner's Office (ICO)[65]. The Information Commissioner herself explained why:

> '*Talk Talk*'s failure to implement the most basic cyber security measures allowed hackers to penetrate *Talk Talk*'s systems with ease. Yes, hacking is wrong, but that is not an excuse for companies to abdicate their security obligations. *Talk Talk* should, and could, have done more to safeguard its customer information. It did not, and we have taken action….In spite of its expertise and resources, when it came to the basic principles of cyber security, *Talk Talk* was found wanting. Today's record fine acts as a warning to others that cyber security is not an IT issue, it is a boardroom issue. Companies must be diligent and vigilant. They must do this, not only because they have a duty under law, but because they have a duty to their customers' (BBC, 2016a, pp.1-2).

[64] The government continues to promote *Cyber Essentials* accreditation as being a crucial part of this, claiming that it will protect businesses 'against the majority of threats on the internet' (DCMS, 2015a, p.3; DBIS, 2015, p.12).
[65] £400,000.

Indeed, within its official report, the ICO stated that this event was likely to cause 'substantial distress' to the many people whose personal data (including banking details) had been hacked (Information Commissioner's Office, 2016, p.7). It also recognised that *Talk Talk*'s lack of vigilance could *facilitate* further crime against those people:

> 'If this information has been misused by the person(s) who had access to it, or if it was in fact disclosed to untrustworthy third parties, then the contravention would cause further distress to the data subjects, and damage [to them], such as exposing them to blagging and possible fraud' (Ibid, p.8).

In its aforementioned efforts to cajole businesses into becoming *Cyber Essentials* accredited, and to purchase cyber insurance cover, the government has sometimes used language which feeds that inference. For example, within a Press Release that accompanied its Report on the role of insurance in managing cyber security risk (Cabinet Office 2015a), the government proclaimed that:

> 'Insurers' support shows the success of the *Cyber Essentials* scheme. They recognise that having *Cyber Essentials* certification is a valuable indicator of a mature approach to cyber security in SMEs, that contributes to the reduction of risk' (Cabinet Office, 2015b, p.2).

Leaving aside its statement about the 'success' of the *Cyber Essentials* scheme (which is highly debatable[66]), the government's choice of words here appears deliberate and precise. Arguably, they carry with them an inference that SMEs who do not yet have *Cyber Essentials* accreditation are, through that omission, acting irresponsibly in relation to their own and others' cyber security.

Recently, such inferences have grown stronger within government discourse. For example, in May 2016 a representative of the Office of Cyber Security and Information Assurance (OCSIA)[67] stated that:

> 'It is absolutely clear in the minds of ministers of this government that company boards, individuals and organisations are responsible for managing this [cyber security] risk. Yes, they need help from government to do that…,

[66] See again section 4.2.2; specifically, page 56.
[67] James Snook, Deputy Director for Business, Crime and Skills, OCSIA, Cabinet Office.

but that responsibility doesn't sit anywhere else, the liability doesn't sit anywhere else' (OCSIA, 2016).

A week later, this frustrated tone re-emerged in a speech given by the Minister for the Cabinet Office, who complained that:

> '[O]nly half of the businesses that we surveyed this year have taken steps to identify cyber risks. Make no mistake, the next data breach will happen. It's your duty to make sure that it's not your company splashed across the [news]papers when it does' (Cabinet Office, 2016a, p.3).

### 4.3.2 Victim Blaming

With the government 'steering' in this way, others have been 'rowing.' In this section, I will provide examples of responsibilisation and the shaping of victim status *in action*. These are case study examples showing how such things are being practised by two of the larger societal institutions in the UK (banks and the police).

At times, the landscape of responsibilisation can resemble shifting sands. The challenging problem of internet banking fraud is just such an area, and continues to provide evidence of how use of the 'ideal victim' stereotype can result in victim blaming. Increasingly, banks have tried to avoid responsibility by blaming customers themselves for their own losses. In 2012, while giving expert evidence to the House of Commons Science and Technology Committee, Prof. Peter Sommer[68] observed that: 'Good advice is provided on Banking sites, but you get the feeling that the banks are trying to minimise their responsibilities in these areas' (House of Commons Science and Technology Committee, 2012, Ev.3). The following year, during his expert testimony to the House of Commons Home Affairs Committee, Prof. Ross Anderson[69] pointed out that:

> '[While] the banks claim that they will blame people [only] if there was gross negligence, in practice they often blame people as a routine matter, even when it is not clear there was negligence at all' (Ibid, Ev.25).

[68] An expert in the digital forensic investigation of cybercrime, and Visiting Professor at the London School of Economics and Political Science.
[69] Professor of Security Engineering at the Computer Laboratory, University of Cambridge.

He then explained further the context in which this occurs: 'Everybody is trying to push liability on [to] everybody else. It is even fashionable in the industry. We call it leverage' (Ibid).

This trend of victim blaming within the Banking sector is not new (MacEwan, 2013), and continues to grow. Indeed, recently Britain's then most senior police officer, Sir Bernard Hogan-Howe[70], suggested that consumers should not be refunded by banks if they fail to protect themselves from cybercrime. He said that customers who had fallen victim to online fraudsters were being 'rewarded for bad behaviour' (Grierson, 2016). His opinion was criticised by many, including the Executive Director of the consumer association *Which?*, who reported that when, in the previous year, they had investigated the matter they found that: 'Too often banks were dragging their feet when dealing with fraud' (Ibid). He said that: 'The priority should be for banks to better protect their customers rather than trying to shift blame on to victims of fraud' (Ibid).

The Fraud Advisory Panel considered that Hogan-Howe's comments came 'dangerously close to blaming the victim, which is unhelpful in the fight against fraud,' and '[took] little account of how cunning and sophisticated fraudsters can be in preying on UK consumers and businesses' (Fraud Advisory Panel, 2016, p.1). Another critic was the aforementioned Prof. Anderson[71], who wrote a letter to *The Times* in response to the Met Commissioner's comments, describing them as 'secondary victimisation.' Therein, he argued that:

> 'Thirty years ago, a Chief Constable might have said that Rape victims had themselves to blame for wearing nice clothes; if he were to say that nowadays, he'd be sacked. Hogan-Howe's view of bank fraud is just as uninformed, and just as offensive to victims….Much of the blame lies with the banks, who let the users of potentially infected computers make large payments instantly, rather than after a day or two, as used to be the case. They take the risk because regulators let them dump much of the cost of the resulting fraud on customers' (Anderson, 2016, p.1).

[70] Commissioner of the Metropolitan Police.
[71] See again note 69.

Two forms of internet banking fraud have become prevalent. The first involves criminals gaining access to individuals' bank accounts after posing as a member of the banking staff. It has been observed that:

> 'In these cases, the banks' default position seems to be that the customer has done something wrong – by answering phishing emails or by being careless with their personal data' (Collinson, 2016, p.1).

Again, however, many of them are reported to be sophisticated scams, 'catching [out] even the most savvy online consumer' (Collinson, 2016, p.1; Fraud Advisory Panel, 2016).

The second form of fraud involves a victim (individual or corporate) who has employed a legitimate builder or similar tradesperson. Criminals hack into the victim's email account, or into the tradesperson's email account, and then send the victim an 'invoice,' purportedly from that tradesperson. Usually, it is for the correct amount. Unsuspectingly, the victim then pays the 'invoice,' using the bank account number and sort code supplied with it.

There are a growing number of these cases. Many of them feature responses from banks that rely on the 'victim precipitation' narrative. For example, a Judge and his wife lost £5,040 to fraudsters who had hacked into the email account of a landscaping company that had done some work for them. Despite the sophistication of this scam, the Bank did not reimburse them. Speaking to *The Guardian*, the victim said:

> 'I am a Judge, and for that reason do not wish to be named in the publicity. But it does mean that I have some familiarity with the law, and it seems to me that [the Bank] owes a duty of care to people whom it knows could be victims of fraud, and that duty is breached if procedures for setting up accounts are foreseeably inadequate, and [breached] again when the Bank allows payments to be made without cross-checking the name of the payee with that of the account holder.' He went on to say that he believed a class action against the Bank 'would have, at least, some chance of success' (Jones, 2016, p.2).

Another example shows more clearly how banks are using the aforementioned narratives to shift responsibility and escape liability. In 2016, a small publishing

business lost £16,790 to fraudsters in a similar way. The criminals hacked into the email account of the firm's Director and, while he was away, sent messages (purportedly from him) to a member of his staff, requesting money transfers to certain Bank accounts. The next day, after realising what had happened, the Director contacted the Bank. Later, the Bank informed the Director that it had been able to preserve some funds before they were withdrawn by the fraudsters. However, these 'preserved funds' amounted to just £26.59. Yet, it was the Bank's accompanying 'offer' that summed up its opinion on the matter, and its attitude towards the business victim: it told the Director that in order to claim this £26.59 he would have to agree to accept it as full and final settlement of all claims against the Bank, and also sign a confidentiality agreement (Jones, 2016, p.2).

A third example illustrates how banks are distancing themselves from any responsibility by using the 'ideal victim' standard when judging the behaviour of those who have been defrauded. In 2016, a record label manager and her husband – described as 'hardly the types you could accuse of not being internet savvy' (Collinson, 2016a, p.1) – also fell victim to this sophisticated type of email scam, losing £25,000. However, their Bank declined to accept any responsibility, on the grounds that the transfer was made by them (the couple), and the Bank was 'merely following their instructions' (Jones, 2016a, p.2). It also told them that it had been unable to obtain a return of the funds from the other Bank (which operated the account used by the fraudster). The other Bank wrote to the couple, explaining that, by the time it was alerted, the couple's £25,000 had been 'utilised' by the account holder, so it was unable to return any of their money. In that letter, it also stated that it does not report scam claims to the police because 'the bank is not a victim' (Jones, 2016a, p.2).

These case examples have concerned cyber security within internet banking, yet the themes and practices they reveal are not peculiar to that sector. Certain dangers lie within responsibilisation, whenever and wherever it is employed. For instance, victim status can be elusive where that status has been shaped by claims of 'victim precipitation' and the use of the 'ideal victim' yardstick. In this way, all claims to victimhood become questionable. In the internet banking fraud cases just mentioned, those who had been defrauded were denied victim status because the banks took the view that their behaviour had not been risk-averse. Such judgements and practices can amount to, or lead to, victim blaming, which is often done to divert attention

away from those people or organisations that are truly culpable. The motives behind such deflection include the avoidance of litigation, insurance payouts, financial penalty, damage to reputation, and loss of business. Consequences flowing from victim blaming can be moral (e.g. injustice) or practical (e.g. worsening a problem by kicking it into the long grass). As the pressure for responsibilisation within UK cyber security grows, the temptation to shape and deny victim status, and to participate in victim blaming, could also grow. In this chapter, I have provided evidence that such blame-gaming has begun in some areas. Yet increasingly, it could be played across the field, by government towards businesses, by businesses towards their businesses partners (e.g. supply chain), and by businesses towards their own employees. And such victim blaming could further undermine the government's recent push 'to use insurance as a driver for improving cyber security practice in UK businesses' (Cabinet Office, 2015a, p.2), because even businesses which have regularly paid in may not get an insurance payout following an incident of cybercrime, if judged as being insufficiently risk-averse.

### 4.4 Conclusion

'Governing' is said to concern the 'conduct of conduct' (Foucault, 1982). In the UK, during the last 30 years the State has moved from a 'sovereign' style of governing by top-down command to one of 'governmentality' (Foucault, 1978), characterised by 'the enlistment of others, the shaping of incentives, and the creation of new forms of co-operative action' (Garland, 2001, p.125). During this time, Neoliberal politics have imposed a form of market rationality on governance (Brown, 2006), involving a culture of heightened individualism and responsibilisation (Brown, 2006; Hall, 2004; Grossberg, 2005). Now, the downsized State responsibilises citizens and organisations with certain tasks, shared to a greater or lesser degree with itself. One of these is the prevention of crime.

My documentary analysis has shown that the UK government continues to allocate responsibility for cyber security to organisations other than itself, particularly businesses in the private sector. In so doing, it also passes to them (most of) the tricky task of responsibilising individuals. Gradually, the language and tone in which the government has done this has simultaneously been shaping victim status. The government realises that cyber (in)security is one of the most difficult risks to manage, and considers this best done mostly by others. Ironically though, that has led to a

situation where, from afar, it is becoming increasingly frustrated with what it sees as poor risk management by those others. In turn, this has caused the government to speak in more judgemental and less tolerant terms on this matter.

My analysis has also brought to light how deeply enshrined Neoliberal conceptions of responsibility and victimhood are within government discourse. Such discourse can be misleading. Within it, the concept of 'victimhood' is often portrayed, through stereotype, as being simple and clear-cut. In reality, it is far more complex (Fattah, 1991; Christie, 1986). Also, Risk 'is never the dry, technocratic matter that it initially appears' (Loader and Sparks, 2002, p.95), and risk management always brings with it a blaming system (Sparks, 2001; Garland, 2001). Cyber security is no exception. In the aftermath of attempted or successful cyber attacks, questions around individual and corporate victimhood necessarily arise. Those questions can be raised in-house (e.g. during disciplinary proceedings) or elsewhere (e.g. during investigations, or in court). Organisations and individuals, including those whose duties include the responsibilisation of others, are expected to justify their decisions or (in)actions. They are held to account. This then ushers in the concept of blame, and with it the danger of misplaced blame, which is much greater given how difficult, if not impossible, it is to gain *legitimate* victim status. Potentially then, all claims to victimhood can be undermined. Indeed, it seems clear that 'the increasingly pervasive aspects of Neoliberal ideology [such as here, responsibilisation] appear to intersect with traditional notions of victim blaming' (Rees and White, 2012, p.429).

For organisations and individuals alike, the consequences of being blamed are becoming more serious as the pressures within and around cyber security increase. In particular, the arrival of the EU's General Data Protection Regulation (GDPR) in May 2018 could have a profound effect, in several ways. This is despite the UK's departure from the European Union, because the government has already stated that it will create legislation to replace the EU rules on data protection (DCMS, 2016). Given this, it seems likely that the UK government:

> 'will want to adopt national laws identical or similar to the GDPR, in order to persuade the [European] Commission that the UK provides an adequate level of protection [within international data transfers]' (Heward-Mills and De Fonseka, 2016).

Also, whichever trading relationship the EU and the UK adopt, 'the extra-territorial reach of the GDPR means it is likely to remain relevant for many UK businesses for years to come' (Ibid), because UK businesses targeting data subjects in the EU could still be subject to fines for not complying with the GDPR. Specifically, it will impose upon organisations more onerous duties concerning data protection, including the legal requirement to notify individuals (and government) of cyber security attacks that compromise personal data and are likely to result in a risk to people's rights and freedoms. Failure to give such notice could bring heavy financial penalty – up to €20 million (£18 million), or 4% of annual worldwide turnover, whichever is the greater (Art.83, GDPR).

Indeed, recently the government reiterated its intention to implement the GDPR (HM Government, 2016c; DCMS, 2017c). In turn, these things will increase the likelihood of UK organisations seeking protection through cyber insurance, urged on by the government (Cabinet Office 2015, 2015a and 2016a). That will then bring additional pressures to obtain, and retain, sufficient cyber insurance cover, which will likely involve obtaining, and then retaining, some form of cyber security accreditation (e.g. *Cyber Essentials*, *Cyber Essentials Plus*, or ISO 27001).

Facing a greater range and potency of threats to cyber security, more onerous legal duties and potential litigation, and the need to remain insured against such things, organisations will place considerably more pressure on all of their employees to comply with cyber security policies, all of the time. The government seems to view this as a difficult, *if somewhat uncomplicated*, task. Whilst often conceding that the responsibilisation of individuals is demanding, the government has continued to signpost a seemingly *straightforward*, if arduous, path to achieving it: inform and train users, and monitor, restrict and discipline user behaviour. But has the government underestimated the complexity of this pivotal task within the human aspects of cyber security? In the following two chapters, I will investigate whether, and how, people follow cyber security rules; and if not, why not? This will involve the presentation of findings from the second and third stages of my research.

# Chapter 5: Case Studies

## 5.1 Introduction

It is now widely agreed that cyber security is composed of three key elements: People, Processes and Technology (Dhillon and Backhouse, 2001; Smyth, 2015; Edwards, 2016; Parent and Cusack, 2016). Crucial to that definition is the deliberate order in which those elements are listed, giving great importance to human aspects. As evidenced in the previous chapter, the government continues to responsibilise businesses for their own, and others', cyber security. This includes the demand that businesses responsibilise each of their employees, and it has told businesses how to do this. On government paper then, this task seems demanding and onerous, yet relatively *straightforward*.

In this chapter, I will investigate whether *in practice* – through training and policy – small businesses have been trying to govern their employees' behaviour in the way that the State has told them to; and if so, how difficult and how effective that has been. This will involve presenting results from my case studies. These will demonstrate that, in a number of ways and for a number of reasons, such responsibilisation of employees is *more complicated* than the government perceives it to be; and that, consequently, it has underestimated this pivotal task.

Three main themes emerged from the data collected during these case studies:

- That employees want guidance on cyber security (section 5.3);
- That there can be a number of problems with guidance through training (section 5.4);
- And that there can be a number of problems with guidance through policy (section 5.5)

Each of these themes, and the evidence supporting them, will be discussed in turn[72].

[72] In these case studies, to preserve the anonymity of the research participants, each person was allocated a number, and each of the three businesses was allocated a letter. Consequently, when data is reported in this chapter and the next, the following abbreviated terms will be used to indicate from which participant the data has come, for which business they were working, and in which stage of the case study they provided the data: P = Participant; A, B or C = the relevant Business; DS = Diary Study; and Int = Interviewing. So, for example, a participant would be quoted/labelled in the following way: 'I don't think there is a specific policy in place at the moment' (P20/B/Int).

## 5.2 The government's own attempts at guidance

Before reporting the experiences and practices of these three businesses and the people they employ, some results concerning the government's own efforts to educate people and businesses on cyber security must be mentioned. They evidence the difficulty of the responsibilisation task, and indicate that the government continues to underestimate it; or, conscious of its own limitations, feels ambivalent towards it.

During the second stage of my case studies, each of the twenty-eight participants were asked whether they knew of the government's *Cyber Streetwise* campaign. Twenty-five of them were unaware of it. Of the remaining three, one said they had heard of it but did not know what it was (P7/C/Int). Another said they had seen it advertised on a billboard poster, but explained their reaction to this:

> 'I scoffed at it. I think I had just seen it after the government had had some huge data leak of some sort or another, and I thought it was a bit rich [for them] to be telling everybody else [what to do]' (P1/A/Int).

The third person said that they had visited the *Cyber Streetwise* website, but added:

> 'I should also point out that I only discovered the website because I was searching for cyber security information online – I was looking for some free educational posters – and I found [a link to] it on a government website' (P18 (IT Manager)/B/Int).

Those twenty-eight participants were also asked whether they knew of the government's *Cyber Essentials* scheme. Only one of them was aware of it (P18 (IT Manager)/B/Int).

Collectively, these results indicate strongly that – in the small business sector, at least – the government's efforts to educate people and businesses on cyber security have been failing. Ironically, this seems to have been due to poor communication of the guidance given through the educational campaign (*Cyber Streetwise*) and the accreditation scheme (*Cyber Essentials*). It has not been promoted and disseminated

effectively. A further irony is that the *Cyber Streetwise* campaign's name has now been changed to *Cyber Aware*[73].

### 5.3 Employees want guidance on cyber security

Some research continues to cite users' *apathy* and *resistance* among the prime reasons for information security breaches and incidents (e.g. Safa and Maple, 2016). Such claims sit within a wider context of contention, which is the long-running debate on how humans should be viewed and understood within information security and cyber security. In my case studies, participant anonymity gave employees the opportunity to speak freely about whether, and why, they might be unreceptive to guidance on cyber security. Each of the twenty-eight participants was asked whether they thought that their work colleagues would welcome more formal guidance on cyber security. Use of the phrase 'formal guidance' invited their views on more training, more policy, or both.

Assumptions about employee apathy and resistance are easily made. Given this, it is interesting to note how the people at the top of these businesses responded when asked whether their employees would welcome more guidance on cyber security. The owner of Business A answered: 'I would hope so. But the plan is to give it to them, anyway' (P1/A/Int). The Chief Executive of Business C expressed a similar view, but more strongly: 'I think they would. Frankly, as the CEO, I don't care whether they would or not; they're going to get it' (P4/C/Int).

In fact, the vast majority of the other participants (23 out of 26) thought that such guidance on cyber security *would* be welcomed. Of the three who thought it would not, two recommended that any more guidance should instead be given *informally*, with one saying:

> 'I think it's useful to be reminded a bit, regularly. And to be updated about what's happening to other businesses, with what's out there. Just keep everyone up-to-date. And not too formally. Just to approach the IT Manager if you have got something on your mind, or something that you're concerned about' (P14/B/Int).

[73] This change occurred in October 2016. See now www.cyberaware.gov.uk

The other said: 'Probably, being nagged on a weekly or monthly basis by the IT Manager is better in many ways [than having more formal guidance]' (P25/B/Int). Only one participant expressed real doubt about whether their colleagues would be receptive to guidance, formal or informal. They said:

> 'Working in this [legal] industry we do need to have all these [training] things. But I don't know whether people are overly enthusiastic about attending all these things. So, I don't know if 'welcome' is the word I would use. But it needs to be done, really' (P21/B/Int).

Among the twenty-three participants who answered 'yes' to the question, sixteen did so unreservedly[74]. For example, one of them explained: 'I think it would just be seen as another round of training, to do x, y and z. These things are an inevitable part of modern day office life' (P28/B/Int). Of the remaining eight, one answered conditionally, saying: 'As long as it's understandable and usable. It's not about whether we all welcome it or not' (P11/C/Int). The remaining six answered cautiously[75]. For example, one of them said: 'I imagine there are a few people who would rather just have their head in the sand, and I don't think they'd welcome formal guidance on anything, let alone cyber security' (P16/B/Int).

Collectively, these results show that almost all of these employees would be receptive to further guidance on cyber security, and that most would not mind it being delivered to them *formally*, through more training and/or policy. The results also indicate that – in these three businesses, at least – most employees feel neither apathy nor resistance towards the *concept* nor the *prospect* of such guidance. Instead, they welcome it. However, their opinions regarding the *detail* of it – its content, form, extent and means of delivery – is another matter, which will now be discussed.

### 5.4 Problems with training

It has been claimed that education can awaken people to the danger in their actions (Besnard and Arief, 2004; Parsons *et al.*, 2010). The main aim of training is to effect *change* in that behaviour. However, change depends also on the existence of a 'security culture' (Sasse and Flechais, 2005). Overall, my case studies revealed that

[74] P2/A/Int; P5, P6, P7, P8, P9 and P10/C/Int; P13, P17, P19, P20, P22, P23, P26, P27 and P28/B/Int.
[75] P12, P15, P16, P18, P24 and P29/B/Int.

differing amounts and types of formal training in cyber security had been given to the employees in these three businesses. Notably, the difference was not just *between* businesses, but sometimes *within* them as well[76]. So, absence of training was not the only problem. Where training existed, it was also problematic, in a number of ways and for a range of reasons.

### 5.4.1 Financial pressure

Training is much determined by monetary cost (Busch *et al.*, 2016). In two of these three businesses, acute financial pressure had influenced heavily the form and extent of the cyber security training given to employees.

The consistently poor financial health of Business A meant that formal training in cyber security had never really featured in its spending plans. The owner explained:

> 'This business has been losing money ever since I set it up, so I've constantly had to put money into it to keep it going….Actually, the corporate work that I do subsidises the business. So, that's the situation. But that can't go on indefinitely, and so that means that we [the company] are under quite heavy financial pressure the whole of the time' (P1/A/Int).

Consequently, cyber security training had been almost completely absent. The owner explained further:

> 'We had a consultant come in and do an audit, and he fed back some areas of weakness. As a result, one of the [former] employees, X, went on a training course [on Data Protection], but he's left now…The only training that's taken place is that one-day course that I sent X on. That's it' (P1/A/DS and Int).

Clearly, the poor financial state of the business was continuing to restrict expenditure on training. Indeed, only one of the three people working for Business A had received any formal training in cyber security, but not from his employer. He was an Apprentice, and had gained some training during his part-time college course (within the Apprenticeship Scheme). However, he did not participate in the second stage of the case study because the day before it was due to start he was dismissed by the owner of the business. Ironically, this was because he was said to have committed

[76] For example, in Business C the formal training experiences of the employees varied considerably.

two separate breaches of cyber security, each of which could have brought serious consequences to the business, such as the extortion of money via the encryption of key data[77]. Indeed, the owner explained:

> 'If I had a Ransomware attack now, I would probably close the business….Because this business is dragging itself out of the mire, and it has been for years, really. So, some serious setback could be enough to tip the balance in favour of just wrapping it all up' (P1/A/Int).

The owner questioned how that person could have worked for the business for over three months without understanding the danger of his actions in both of those situations. However, he then went on to say:

> 'But, you know, there's a question I'm asking myself: Is it something to do with how we trained him, or is it just that he hasn't got the nouse to really understand these kind of issues? And I think it may be a bit of both' (P1/A/Int).

In this way, he conceded that problems with training had been, at least, a significant cause of those cyber security incidents. Indeed, all of his comments pointed to a further irony: that, necessarily, a really tight rein was kept on spending in this business, but little or no expenditure on cyber security training was putting the very existence of the business at constant risk.

It seemed that any training (on anything) within Business A was given *informally*. That heavy financial pressure on the business made time even more precious. Selling and servicing took priority over formal training. Also, with the business employing just three people – one of whom (the owner) would be the trainer – any formal training sessions would have taken, at least, two-thirds of the workforce away from those other key tasks for periods of time. Again here, formal training was losing out to business survival in the 'prioritisation wars' (P1/A/Int). This chimes with claims that crime is not a priority for most of the non-State agencies that are capable of doing

[77] Specifically, this former employee (P3/A) was said to have done the following two things: a) Instead of giving the login details of a dummy hosting account to a company based in India (for them to work on it), he gave them the login details for an entire re-seller account (comprised of 30 individual web hosting accounts); and b) On another occasion, one of Business A's clients (for whom they host email) telephoned to ask that the email account of one of their employees (who was just about to leave their employ) be locked, so that she could not delete emails within it. Instead of locking it, by mistake P3 actually deleted the whole email account in question.

something about it (Garland, 1996); and that, usually, such organisations (e.g. Business A) will concentrate on primary objectives such as the delivery of services and business survival without much concern for crime, provided that the experience/cost of crime does not directly and substantially interrupt those primary activities (Pease, 1994). The physical size and layout of the workspace within Business A – again, restricted by monetary cost – may have been influential here as well. All three employees worked in the same small open-plan office. This close physical proximity invited the compromise of *ad hoc* informal training, given alongside or between the key tasks of selling and servicing during the working day.

As a charitable organisation, Business C also keeps a very tight rein on expenditure. Again, financial pressure has influenced the provision of cyber security training to its staff. Overall, the employees' responses indicated an absence of *organised* training. In fact, their individual experiences of formal training varied considerably. One person confirmed that they had received no training (P9/C/DS). Another reported that they did not think that they had (P7/C/DS). A third said that they *had*, but could not remember anything about it P11/C/DS). Another person mentioned receiving only one piece of formal advice on cyber security, which was when the Office Manager told them not to accept web browser prompts (P6/C/DS). Four other participants all reported receiving some formal training, but not always of the same degree or type. For example, the Chief Executive of the business explained: 'We have received guidance from our IT support provider. The format has varied: email, telephone, face-to-face, and web-based' (P4/C/DS). Somewhat differently, the Office Manager reported: 'We were given induction training on how to use spam filters and safe password use. Our IT Support provider gives *ad hoc* advice, which is conveyed to staff by email' (P10/C/DS). Such disparity of provision, and of recollection[78], was caused in no small part by a lack of available money. Again here, poverty made survival the first priority of this business; and, as in Business A, the *organised* provision of staff training in cyber security was more of an aspiration than a plan.

A wider observation can be made here as well. Often, financial pressure on *small* businesses is both constant and intense, as evidenced in these case studies – particularly, within Businesses A and C. This makes it less likely that they will comply

[78] Providing further evidence of the problems of 'training fatigue' and 'security fatigue' that will be discussed in section 5.4.3.

with demands for them to reach, and then *sustain*, acceptable levels of cyber security in their day-to-day operations. Such demands come from other businesses/organisations with which they trade or communicate, from insurance companies, and from government. In turn, that increases the risk that victim blaming might occur.

### 5.4.2 Pitching to training needs

Humans differ, not least in their knowledge and experience. That difference complicates the task of training them *all* in matters such as cyber security, because they have dissimilar training needs. For example, an employee in Business C reported being frustrated by the fact that there was a wide range of computer literacy among their colleagues, which meant that any training was necessarily pitched at low(est) levels:

> 'There is a lack of knowledge…And particularly with some people who perhaps aren't as computer literate as others. We had quite a long – in fact, arduous – training session [about using] *Twitter*, so that's the kind of level' (P6/C/Int).

Another participant corroborated this point about computer literacy: 'I think that quite a lot of my colleagues are not particularly IT-savvy. Some are, but plenty aren't' (P5/C/Int). This brings a risk that if information is pitched at particularly low levels, some people may be dismissive of it, and begrudge the time spent receiving it. However, sometimes even the pitching itself can be wrong, particularly when parts of the training are conducted via email (sent to all, collectively) rather than in person (e.g. in training workshops). This particular problem was being experienced by one of the employees in Business B, who reported that: 'A lot of [the IT Manager's] emails are in IT language,….and a person like me doesn't really understand that, anyway, if I was to read it. I just think that it goes over your head a little bit' (P24/B/Int). For this person, the training had been pitched too high.

Ideally, each person's cyber security training would be tailored to their own level of knowledge and experience. Indeed, research has shown that training can be especially effective when personalised (Mangold, 2012). However, such bespoke provision is likely to be more expensive and, for reasons already explained, small businesses such as these tend to be very cost-conscious.

### 5.4.3 'Training fatigue'

Several participants reported experiencing what might be termed 'training fatigue.' This is where they become weary of, or frustrated with, attempts to train them in cyber security, which can result in them being much less responsive to such training. Here, parallels can be drawn with 'security fatigue' (Furnell and Thomson, 2009a; Stanton *et al.*, 2016), where people tire of security procedures and processes, often because of 'friction' with their primary work tasks, caused by an imbalance between security and usability (Beautement *et al.*, 2008; Bada and Sasse, 2014).

Perhaps surprisingly, given that it is a law firm, formal training in cyber security was also somewhat absent in Business B, although less so than in Businesses A and C. This was despite it being the only one of these businesses to employ an (in-house) IT Manager. Six of the eighteen participants reported that they had *not* received, or could not remember receiving, any such training whilst working for the Business[79]. Eleven of the participants reported that they *had*, through verbal and written communications from the IT Manager[80]. These different recollections can be explained. Within that first group of six people, some did not recognise that those communications were deemed by the IT Manager to *be* training, and others simply did not engage with it (e.g. choosing instead to ignore or delete such emails), perhaps because of 'friction.'

One participant did give more detail on the degree of formality and regularity of this training: 'We have emails sent to all staff by [the IT Manager], and occasional meetings where the subject is brought up [by him]' (P19/B/DS). When asked in interview whether he thought that Business B's employees would welcome more formal guidance on cyber security, the IT Manager himself said: 'I think that they would like to gain more knowledge on it, without having to put a lot of effort into doing so' (P18 (the IT Manager)/B/Int). This was interesting. It seemed to explain the chosen nature and form of the existing training (delivered only by him, and mainly via email), which sought to be informative but not too onerous or intrusive.

So, any cyber security training within Business B was delivered by the IT Manager. Usually, this consisted of him emailing information to all employees (e.g. to warn them

[79] P17, P20, P21, P22, P23 and P24/B/DS.
[80] P12, P13, P14, P15, P16, P19, P25, P26, P27, P28 and P29/B/DS.

of new threats, and to recommend or reiterate good cyber security practices). Sometimes, he would give such information to them verbally as well (e.g. for a few minutes within a quarterly staff meeting). However, the case studies revealed a number of problems with these approaches, many of which involving forms of 'training fatigue.' One participant reported that the IT Manager was himself aware that his approach was failing. He explained:

> 'To some extent, [the IT Manager] is doing a good cop, bad cop all by himself….And sometimes he's trying to make an impact – because he doesn't feel that people are engaging with it – and sometimes what he is doing is pushing people further away.….It's difficult, because he wants to get a response from people. And there's a little bit of the sports mindset of: 'I want to make them angry, so that they perform properly.' But that doesn't work for everyone' (P16/B/Int).

Indeed, during interview many of the participants confirmed that this approach was failing. The use of email for the purposes of training drew much criticism. As one participant put it:

> 'I know from experience that when the IT Manager sends around emails about stuff like that [cyber security], they generally just don't get read…people choose not to read them. I know that within his emails he says: 'Please *do* read this, and *don't* ignore it.' But I'm sure that a lot of people do just still ignore them' (P24/B/Int).

A number of other participants confirmed that this was a recurrent problem in Business B[81]. These responses also support research findings that when the same stimulus (e.g. email) is used repeatedly to convey a concept (e.g. cyber security), employees are prone to ignore that stimulus (Furnell and Thomson, 2009).

In Business C also, similar views were expressed on the problems of using email for training purposes. For example, one participant said that: 'If an email [on cyber security training] comes in, I don't always have time to spend and take it in' (P8/C/Int). Another suggested that such training emails are given, at best, only cursory attention:

[81] P12, P15, P17, P20, P21, P24, P26 and P27/B/Int.

> 'We can click it and skim read it in ten seconds, and then just get back to our work. But if you pull people away from their desks, they *are* going to listen, they *are* going to understand. They've then got the time to take it in, digest it' (P9/C/Int).

Naturally though, the efficacy of any different form of training will depend, in turn, on matters already mentioned, such as its content, to whom it is pitched and how, how regularly it takes place, and for how long each time. Again lurks the potential both for 'friction' and 'training fatigue.'

Cyber security is a form of risk management. However, risk management *itself* presents a danger of people or organisations becoming overburdened by it (Bauman, 2006). One of Business B's employees confessed to feeling decidedly uneasy about the issue of cyber security, and training related to it: '[A]t the moment, I find the whole thing quite daunting. And you can become quite overwhelmed by it, and quite scared by it' (P29/B/Int). This issue was touched upon by another person, who explained how it can also lead to a different problem:

> '[T]here is a growing awareness, and people are scared of it [cybercrime]. So, the more you hammer it [the cyber security message], the more scared of it they become, and that doesn't necessarily help. So, I think sometimes you can overplay it. Not overstate its value or importance, but just in terms of the buy-in that you get from the staff, if you hit it too hard, too often' (P16/B/Int).

Again, these can be seen as forms of 'training fatigue.' Another was reported by someone else in Business B: 'I almost think that people just get a little bit bored of hearing about the same thing, like all the time. Then people start to switch off a little bit, and it's like you're constantly being given all this information' (P24/B/Int). This point was made also by someone in Business C, who said: 'There's a danger of kind of overloading people with guidance, that ends up being ignored because it's just too much' (P5/C/Int).

### 5.4.4 Training preferences

Given how problematic the participants' training experiences had been in each of these businesses, it was important to ask each of them what would be the best way to deliver cyber security training to them, personally. On this question, there were more

instances of shared or similar opinions. However, there was still a considerable range of views, and the answer of a participant in Business A included his idea of why this might be:

> 'Everyone works differently. Everyone's mind works differently. Whilst I'm technologically able, I'm not a techie, if that makes sense. And I think there's a subtle difference. And, as a result, I think a lighter level of cyber security awareness, maybe, would be useful [to me], just to keep an eye out for tricks and whatever, beyond the sort of stuff that you pick up as you go along' (P2/A/Int).

Among the remaining twenty-seven participants, sixteen[82] thought that (face-to-face) workshops, in small or larger groups, would be the best way of delivering such training. Sometimes, opinions differed on the form that these workshops should take. Also, some people envisioned multi-faceted workshops while others preferred ones with a single theme or activity. But overall, several common themes emerged from their answers. Seven[83] of those sixteen people specified that in these sessions they would welcome presentations by people from within or outside the business. The same people and others[84] said that they would value the opportunity to discuss cyber security issues, problems and experiences with their work colleagues. As one of them explained:

> 'We've recently had some workshops [on other matters]…and I actually really enjoyed them for the opportunity to get together with the other members of our team, and to discuss problems which we are all facing' (P6/C/Int).

A number of them[85] also stressed the importance of using examples in these training sessions, particularly real-life examples.

However, the twelve other participants held rather different views. Five of them[86] thought that such training could be delivered, either occasionally or regularly, within staff meetings. One person[87] expressed a preference for one-to-one guidance. In

[82] P1/A/Int; P4, P6, P8, P9, P10, P11/BC/Int; P12, P19, P20, P21, P22, P23, P26, P28, P29/B/Int.
[83] P4, P8/C/Int; P21, P23, P24, P28, P29/B/Int.
[84] P4, P6, P8/C/Int; P21, P23, P24, P28, P29/B/Int.
[85] P11/C/Int; P12, P19, P21, P22, P28/B/Int
[86] P10/C/Int; P24, P25, P27/B/ Int.
[87] P8/C/Int.

stark contrast, two people[88] said that they would prefer to continue receiving such guidance via email. Interestingly, someone else specified that they wanted methods which would be less time-consuming, and woven more into the working day:

> 'It would have to be something that fits into your day, for which you're not having to do extra work. I don't know whether you could put things around the office; you know, like reminders. Up on the [computer] screen would be a really good idea. Maybe when you log on in the morning? Or it just pops up now and again? Just to prompt you, as a reminder' (P7/C/Int).

Mistakenly, security professionals tend to treat users' attention and effort as if it were an unlimited resource (Herley, 2009). In reality, it is finite. When security measures do not obviously assist users in their work, extra (non-productive) effort is asked of them. Research has shown that, in each instance, users weigh the need for, and benefits of, a security measure against its perceived cost, in terms of that extra effort (Beautement and Sasse, 2009). This determines whether they choose to comply with it. Any expended extra efforts accumulate within their 'compliance budget,' which stretches only so far[89] (Beautement *et al.*, 2008). Note that this assumes that people have interpreted/understood the rules or measures, in order to then weigh up their costs and benefits[90]. Mention of the 'compliance budget' is made here because, beyond that internal cost/benefit analysis, there are a number of external factors which can influence either the size of a person's 'compliance budget' or the rate at which it becomes spent (Beautement *et al.*, 2008), and training is one of them[91].

Naturally, the potential efficacy of training increases when it is delivered to someone in a way of their choosing. But, collectively, these responses reveal how diverse people's views can be on *how* they wished to be trained in cyber security. That diversity itself makes such training even more problematic because – again, for several reasons (e.g. cost, and continuity/coverage of work) – many businesses would baulk at the idea of using a range of bespoke training methods to suit their employees' individual preferences.

---

[88] P14 and P15/B/Int.
[89] To their 'compliance threshold.'
[90] This particular matter will be revisited for detailed discussion in the next chapter.
[91] Including here, the raising of people's awareness of threats (this formed part of the training initiatives within Businesses B and C).

## 5.5 Problems with policy

The main reason why training and policy are so important is that systems' technical vulnerabilities form only part of the cyber security picture. Human error and social engineering complete it (Schneier, 2000). Consequently, it is crucial to consider both the *physical* and *social* contexts in which (fortified) technology is used (Karyda *et al.*, 2005; Beautement *et al.*, 2016). Within that fuller picture, responsibility for protecting an organisation extends beyond its information security experts to each of its employees, who play a key role in the delivery of its cyber security policy (Kirlappos *et al.*, 2014).

### 5.5.1 The existence of formal policy on matters concerning cyber security

At the time of the case studies, none of these three businesses had what could be termed a 'cyber security policy.' However, Businesses B and C did have some formal policy documents on cyber security matters. But, being rather compartmental, these tended to lack connection to each other, or were missing key content. There were also some important issues on which they had no formal policy. In short, within both of these businesses, policy on cyber security was somewhat piecemeal.

In Business A, there existed no formal policies on any cyber security matters. During interview, the owner mentioned again the constant financial pressure that the business was under, and cited this as the reason why policies on cyber security had not yet been written. Commenting that the phoning of a customer or the delivery of a service had always taken priority over such things, he explained: 'It's not that I don't think it's important. But, on the scale of things, it's one of these things that is a job that's constantly getting postponed' (P1/A/Int). At one point, a former employee had been tasked with putting together a data protection policy for the business, but they did not finish this before they left. That unfinished document was shown to me. It was a sample data protection policy downloaded from the web, into which the business's name and other information had been added in handwriting. I was told that it had not yet been used.

As mentioned earlier[92], the day before I conducted the interviews in Business A one of its two employees was dismissed for two alleged breaches of cyber security. When I

[92] In section 5.4.1; specifically, on pages 77-78.

interviewed the other (remaining) employee, he alluded to this while commenting on the absence of cyber security policy within the business, saying: 'I think – particularly with the unexpected turnover in certain roles within the company – that it would be prudent to have a measure of policy [on it]' (P2/A/Int). Interestingly though, he went on to give his opinion on the limitations of such policy:

> 'I think it just comes down to common sense a lot of the time, rather than a rule saying 'you must keep an eye out for this.' Because attacks and viruses could come in all shapes and forms. And you could have a list as long as your arm of things that you could, potentially, keep an eye out for. It's good to be mindful of them, if they're particularly obvious ones that are really easy to spot. The less obvious ones? I think you can only really confront them when they happen, regrettably' (P2/A/Int).

However, here he seemed to be conflating the *need* for policy with its *content*; specifically, by assuming what its content would be, if it existed.

Business B had a number of policies relating to cyber security. In addition to one for data protection, there were policies on use of the internet, the intranet, email, social media and remote working. Although these latter policies were grouped together in one section of the Office Manual, there was little other linkage between them. However, they did share *some* commonality. Much of their content amounted to lists of things that employees must not do, and what action could be taken against them if they did (e.g. disciplinary). In this way – perhaps unsurprisingly within a law firm – they often resembled legal contracts more than cyber security policies[93]. At times, there were notable omissions from them[94]. For instance, there was little advice or information on what cyber security risks to look out for and guard against, in which circumstances, and in what ways. For example, neither the social media policy nor the email policy made mention of the threat of phishing. Also, the business had no formal policy/procedure for reporting risks and incidents which breach, or threaten to breach, its cyber security.

[93] Redacted copies of those policies can be found in Appendix A on page 155.
[94] Judged against standards set, for example, within the government's *Cyber Essentials* scheme and its *Cyber Aware* initiative.

Similarly, Business C had policies on data protection, use of its IT systems, email, social media and remote working. Again, however, these were rather detached from each other. Two of them (data protection and the use of IT systems) were in one document, two more (email and remote working) in another document, and one (social media) in a third document. Overall, compared to the policies in Business B, they featured more content regarding cyber security. However, much of the information within them was about the physical and digital actions to be followed during use of these systems and applications[95]. Again also, the social media policy made no mention of cyber security threats, and the business had no formal policy/procedure for reporting risks and incidents which breach, or threaten to breach, its cyber security. Nevertheless, in comparison to those in Business B, these policies seemed to place more individual responsibility on the employees for the 'cyber hygiene' of the devices that they use. This may be explained by the fact that, unlike Business B, this business could not afford to employ an IT Manager. Consequently, although their IT Support company was readily contactable for advice, more written guidance seems to have been given to employees to compensate for the absence of everyday in-house assistance.

### 5.5.2 Differing awareness and knowledge of policy

Any chance of successful engagement with cyber security policy depends first on the knowledge that it exists, and then knowledge of its content. Beyond that, other matters become crucial[96]. However, research suggests that 'employers can be relatively confident that improving their employees' knowledge of policy and procedures will have a positive impact on both [their] attitude towards those policies and procedures and [their] behaviour' (Parsons *et al.*, 2014, p.174).

Within the first stage of the case studies, each of the participants was asked whether the business for which they worked had the following three types of policy:

- A remote working policy.
- A policy on employees' use of social media.

[95] Redacted copies of those policies can be found in Appendices B (page 166), C (page 171) and D (page 175).
[96] These will be discussed in the next chapter.

- A policy for reporting risks and incidents which (are thought to) have either threatened or breached the Business's cyber security.

**Business A**

The owner of Business A confirmed that it did *not* have a remote working policy. However, one of the two employees did not know whether such a policy existed (P3/A/DS), and the other answered: 'Not a formal policy' (P2/A/DS). There was also some confusion about whether the business had a policy on employees' use of social media. One employee answered: 'I don't think so, but I'm not 100% sure' (P3/A/DS). However, both the owner of the business and the other employee confirmed that there *was* such a policy. Lastly, while all three of them reported that the business had no formal policy for reporting cyber security risks and incidents, one did so hesitantly, saying: 'I don't think so' (P3/A/DS).

**Business B**

Within this business, there was much confusion around the existence of policy. It *did* have a remote working policy, but only four[97] of the eighteen participants knew this, and one of them was unsure of its content. Thirteen[98] of the eighteen participants did not know whether the business had such a policy. The most surprising of the wrong answers came from one of the Directors of the Business:

> 'As far as I'm aware, it does not have one. And that alarmed me, actually, because I tend to write our policies. But it is difficult to know what to put in [such a policy], because we all work differently' (P25/B/Int).

The business had a policy on employees' use of social media. Sixteen[99] of the eighteen participants knew this, but three of them[100] were unsure of its content. The remaining two participants[101] did not know whether such a policy existed. Although the Business had no formal policy for reporting cyber security risks and incidents, four[102] of the eighteen participants stated wrongly that it did. Another person answered (also incorrectly): 'I am sure that there is something in our Office Manual about this, but I

[97] P12, P15, P20, P26/B/DS.
[98] P13, P14, P16, P17, P18, P19, P21, P22, P23, P24, P27, P28 and P29/B/DS.
[99] P12, P13, P14, P15, P16, P17, P18, P19, P20, P21, P24, P25, P26, P27, P28 and P29/B/DS.
[100] P20, P24, P27/B/Int.
[101] P22 and P23/B/DS.
[102] P15, P25, P26 and P28/B/DS.

don't know specifically' (P29/B/DS). Ten participants[103] did not know whether there was such a policy, and just three[104] knew there was not.

**Business C**

Confusion around policy abounded in this business as well. Only three[105] of the eight participants knew that the business had a remote working policy. Two others seemed uncertain, both of whom replied: 'Yes, I think so' (P5 and P9/C/DS). One person[106] did not know whether such a policy existed. Another[107] stated wrongly that it didn't.

The Business had a policy on employees' use of social media. However, four[108] of the eight participants did not know this. Another answered: 'I think so, [but] I am not sure where to find it' (P8/C/DS). Only three people[109] knew that such a policy *did* exist.

Although the business had no formal policy for reporting cyber security risks and incidents, three[110] of the eight participants stated wrongly that it did. Two other people[111] were unsure about this, one of whom commented: 'It may come under ISO 9001[112], but I wouldn't know what to do if it happened to me' (P6/C/DS). Just three[113] of the participants – two of whom were the Chief Executive and the Office Manager – knew for certain that the business had *no* such policy of its own.

Collectively, these responses show that across the three businesses there was considerable difference in the employees' awareness of *whether* formal policies actually existed on some key matters and/or what was their *content*; and such confusion was detected at all levels of employment, from Trainee to Chief Executive. Given this, although there is that link between improving knowledge of policy and thereby improving attitudes and behaviour towards it (Parsons *et al.*, 2014), *first* it must be recognised that improving people's knowledge of policy is *itself* more difficult

[103] P14, P16, P17, P19, P20, P21, P22, P23, P24 and P27/B/DS.
[104] P12, P13 and 18/B/DS.
[105] P4, P7 and P8/C/DS.
[106] P11/C/DS.
[107] P10/C/DS.
[108] P6, P7, P8 and P11/C/DS.
[109] P4, P5 and P10/C/DS
[110] P5, P7 and P8/C/DS.
[111] P6 and P11/C/DS.
[112] This is a set of (certifiable) standards for a quality management system, laid down by the International Organization for Standardization (ISO). See further at http://www.iso.org/iso/home/standards/management-standards/iso_9000.htm
[113] P4 and P10/C/DS.

than it seems. So, confidence in that linked process should be tempered with that particular reality.

### 5.5.3 Disengagement from policy

On its own, awareness of policy brings nothing. Where formal policy is known to exist, *disengagement* from it can be a challenging problem. These case studies found that there are several reasons why this might happen: The amount of existing policies, their content, and the way(s) in which they are disseminated to people can each potentially affect people's engagement with them.

As reported earlier[114], many of the participants in these studies welcomed the prospect of further formal guidance on cyber security. However, some of them also made mention of the increasing *amount* of policy. This can bring with it a risk of disengagement through what might be termed 'rule fatigue' – the danger that people feel pressured by the number of rules, and/or frustrated by the 'friction' they cause with the performance of their primary work tasks. There was particular concern expressed about this within Business B. Therein, one person complained that: 'At the moment, we are being given a lot of new procedures to follow…I mean, it's starting to feel that the job is more like a procedure checklist' (P29/B/Int). Another admitted to having 'huge concerns' about this issue, and cautioned against an 'over-zealous approach' to policy creation (P16/B/Int).

More specifically, there can be tension here between the perceived need for policy and people's concern that it could interfere with their ability to do their daily job; and this can arise, not just from the number of policies, but what is in them. As one participant in Business B put it:

> 'It depends on their content. We're already in quite a heavily regulated industry [the legal sector], and I think it puts quite a lot of people off. Because there are definitely aspects of this job where you feel like you are just doing compliance more than anything. And you kind of think that your job is just going to become compliance; that you will not actually be doing your job most of the time' (P21/B/Int).

[114] In section 5.3; specifically, on page75.

Another person explained that: 'It feels as if you are having more pressure put on you, when it is a very formal process' (P14/B/Int). Two other participants confirmed they were having to do many more cyber security-related checks, 'incurring more time' (P13/B/DS) and 'therefore prevent[ing] us from doing something else' (29/B/DS). Indeed, sometimes employees can feel that their relationship with policy is rather adversarial (Adams and Sasse, 1999). *In extremis*, this can place them in an 'impossible compliance regime' (Herley, 2009).

Also, such tension can lead to errors, and an inescapable truth within cyber security is that just one mistake, by one person on one occasion, can bring serious consequences. A cause of such mistakes can be momentary disengagement from one policy, out of many. For instance, under pressure of time or work (or both), people might forget about, be distracted from, or simply decide not to engage with a particular aspect of a cyber security policy. For example, during August 2016 I conducted a case study of a cyber attack on a small business. It was a Ransomware attack, triggered by one of the employees clicking on a document within a zip file that was attached to a phishing email. They were also on the phone at the time, and said that this had distracted them from thinking carefully about whether the email was suspicious. Two hours later, when they left the office to go home, they forgot to follow another aspect of cyber security policy, by leaving their computer running in the office. Ultimately, this led to that business having to pay the ransom to the cybercriminals, because overnight the Ransomware was able to encrypt many more files that it found on the server, before the offsite backing up process took place[115], and some of those files were crucial to the business.

It seems also that disengagement from policy can result from what might be termed 'reminder fatigue' – the danger that reiteration of policy can deafen ears. As businesses continue to create cyber security policy, they seek regularly to remind their employees of it. Yet, potentially, that reiteration can itself reduce rather than sharpen their employees' focus on policy. These case studies found reasons why people might 'switch off' from this process. Some participants suggested that *too frequent* revisiting

[115] Previously, the business had got very close to their quota on their backup (at their IT Support company). Unfortunately, instead of spending more money to increase that quota, they decided to stop all redundant copies. Consequently, when the local copy of the files became encrypted, they were then backed up (offsite) in encrypted form, with no previous (unencrypted) copies being kept.

of the subject could, paradoxically, corrode attention to it. When asked whether there is a risk of people switching off, a participant in Business B replied:

> 'Yes, there might be. Particularly in my department, because I do Conveyancing. And obviously, we are the most likely target [for cybercriminals]. We *do* talk about [cyber security] *all* the time' (P15/B/Int).

Interestingly, Business B's Marketing Manager commented on that same risk, and warned against:

> 'hitting it too hard all the time, because people will become alienated from the principle, and they will just begrudge it; and that's not helpful. Because the problem that we have at the moment is that, you know, we are having a *lot* of chats about cyber security' (P16/B/Int).

Similar to training here, dissemination of the information can be problematic, which in turn can cause disengagement. Firstly, weaknesses in communication can occur. Some people view some of these as inherent to business generally. As one of the Directors of Business B commented:

> 'I have just disseminated a new policy to my department. I don't know whether it has been disseminated to the rest of the staff. We do act in little, rather *ad hoc* groups within the firm, as I'm sure most businesses do' (P25/B/Int).

Another person in Business B seemed to confirm the existence of this problem:

> 'They [the firm] do have certain [policies concerning cyber security] in place. But I'm not sure that safeguards are necessarily known about *throughout* the business; they are not really communicated that well' (P24/B/Int).

Even where communication to all is achieved, the timing of it can still cause problems. For instance, a participant in Business B explained that: 'If [policy] is thrown in or launched too quickly, then it's immediately going to cause friction' (P23/B/Int).

These case studies also found that the efficacy of policy is determined, *inter alia*, by people's individual preferences for *how* it is delivered to them. But some participants' choices were very different from others'. For example, several people preferred to

receive new policy in *written* form, for them to read later at a time of their choosing. As one participant in Business B explained:

> 'I would prefer it in an email. That's what we tend to do with all our policies. When we've written a new section in the Office Manual, everybody gets emailed on it. And the email either says 'go to this section to print it off,' or it says 'here it is attached for you.' I mean, I personally need a bit of paper. So, I would appreciate an email, and then I can print it off' (P15/B/Int).

Similarly, a participant in Business C stated: 'For me personally, as long as [the email message] was fairly short [and was saying]: 'Here's a new policy, here's what you need to do, here's the detail, go and read it.' That would work for me' (P5/C/Int).

However, there were a number of people for whom delivery of policy via email was much less effective. Reasons for this included people feeling that they didn't always have time to read the email-delivered policy properly, and to take it in (P8, P9/C/Int). Indeed, some people reported giving no more than scant attention to such communications, most of the time. For example, one participant in Business B admitted that '90% of the time' they would 'just quickly scroll through' that type of email (P12/B/Int). Another stated that: 'Even where some of the emails are labelled 'All Staff' or 'Urgent' or 'Must Read' or 'Critical,' I think most people would only skim-read [them], at best, anyway' (P21/B/Int). Furthermore, some people reported that they would simply not read them[116], either because (being busy) they kept putting it off and never finally read them[117], or just because they ignore them on arrival[118]. As one participant commented: 'Emails going out are great, but people just don't read them, and put them into a folder, or delete them' (P17/B/Int). Again here, a number of people were expressing preferences for this type of formal guidance to be delivered instead, or also, in the *spoken* word (e.g. in meetings or workshops). As one of them explained:

> 'It's better to have presentations and stuff, rather than just written formal policies…So, I think it's probably one of those things where it's better to discuss it orally than to have just some written procedure' (P21/B/Int).

[116] P17, P20, P24, P26, P27/BB/Int.
[117] P26, P27/BB/Int.
[118] P17, P20, P24/BB/Int.

Overall then, the participants' views on *how* policy is disseminated, and how it *should be* disseminated, were rather different. Also, crucially, this difference brings with it the danger that some people may be disengaging, either occasionally or continually, from some or all aspects of certain policies – with concomitant risks to the business, and perhaps to others.

### 5.6 Conclusion

In this chapter, some of the findings from the three case studies have been presented and discussed. Collectively, they indicate that the government has underestimated the crucial task of responsibilising individuals for cyber security. In the main, it has delegated this task to businesses. Presumably, the government would argue that such delegation is pragmatic because, for a number of reasons (relational, commercial and practical), businesses are best placed to do it. Yet, as these results have shown, this task is not as straightforward as the government seems to think it is.

Guidance seeks to impart knowledge. First, however, guidance must be *known* to exist. These studies indicate that the government itself has been failing in its own attempts to educate individuals and businesses about cyber security via the *Cyber Streetwise* (now *Cyber Aware*) campaign and the *Cyber Essentials* accreditation scheme, simply because many people and organisations remain unaware of these initiatives. In short, whatever its own practice, the government has been faltering in its preaching.

These studies also found that employees are not necessarily resistant to formal guidance on cyber security, whether through training or policy. Indeed, the vast majority of them said they welcome it. However, it was discovered that *in practice* the *provision* of such guidance can be beset with problems. Training employees in cyber security can be problematic for a range of reasons. Sometimes, financial pressure can preclude or displace plans for it. Necessarily, this can increase the risk of cyber attack[119]. Also, the training needs of the employees can differ significantly. This brings with it certain tensions. If the same training content is delivered to all, in the same way, and at the same rate, this may cost less financially. But some staff – who consider that training too basic or too slow – may begrudge it because they view it as

[119] For example, the delivery of Ransomware via phishing emails.

wasted time in their otherwise busy working lives. Among other things, this can undermine efforts to create, and sustain, a culture of cyber security within an organisation.

The participants in these case studies also reported experiencing some forms of 'training fatigue.' Unnecessary use of 'IT language' could distance some people from the process. Information overload might cause others to 'switch off,' and too frequent training, or 'overplay'[120], could make some people anxious, either through fear of the now known or unease that training was cutting into their worktime. This research also found that people's individual preferences for *how* they should be trained, and what should *feature* in that training, differed significantly. Again, this brings back the matter of cost. Catering to all (or most) of the training preferences of their employees might promise to increase the efficacy of training, but small businesses such as these will be loath to pay for it, unguaranteed.

These studies also found evidence that guidance through policy can be problematic as well. One of the businesses had no formal policy on cyber security. It had been struggling to survive, and such policy was not seen as a priority. The other two businesses had some policies but not others, and those that existed tended to lack connection to each other. First, however, there was a problem with awareness of policy. This was found in surprising degree throughout these two businesses. Many people did not know that certain policies existed, let alone their content. Of course, sometimes one might be unaware of a rule but still be 'following' it. For example, a tourist may not know of the rule that people should stand to the right on escalators within the London Underground system, but by observing and matching the behaviour of others they act in accordance with the rule. However, in situations without such social signposting, there exists a danger that people may practise their *own* policy, thereby weakening cyber security. Furthermore, the studies also found that where people *are* aware of policy, there are several reasons why they might still *disengage* from it. Again, individual preferences for how the policy should be delivered to them seemed to play a very significant role here. Also, some people reported experiencing 'reminder fatigue,' induced by what they saw as a bombardment of communications on cyber security. This could cause them to feel alienated from that subject, or simply

[120] A term used by one of the participants. See again the comments of P16/B/Int at the end of section 5.4.3.

to ignore it – for a while, at least. These and other such tensions increase the risk of mistakes and other insecure behaviours.

These findings have shown that governing people's behaviour around cyber security in (and beyond) the workplace can be far from straightforward, due mainly to cost and 'friction.' However, in the next chapter I will demonstrate that these problems are just the tip of the iceberg, and how this task is *even more difficult* than has been recognised before.

# Chapter 6: Rule-following

## 6.1 Introduction

In the previous chapter, I provided evidence that the government has underestimated the difficulty of responsibilising individuals for cyber security; a task which, essentially, it has delegated to organisations other than itself[121]. However, the problems I have discussed so far constitute only part of that complexity. In this chapter, I will reveal its true extent.

That delegated task of responsibilisation has demanded also the creation of localised policy. Businesses have been told to form, or assemble, their own rules on cyber security; ideally, set within a 'cyber security policy,' but not necessarily so. For example, it could instead be the collation of a number of policies already in existence (e.g. data protection policy, remote working policy, etc.). The point is that, within this context of responsibilisation, and reflecting the government's instructions to them on this matter[122], each individual organisation is expected to have assembled their own framework of rules for governing their employees' behaviour around cyber security – what I will refer to as their 'rule set.'

Herein, lies something that complicates that task of responsibilisation even further: the issue of rules and rule-following. In this chapter, I will present further findings from my case studies. These will demonstrate the reality of the relation between rules and conduct within the context of cyber security, and shed new light on the matters of whether, and how, people follow cyber security rules; and if not, why not?

The word 'rule' can be 'an especially messy cluster concept' (Lewis, 1969, p.105). So, it is important to note that within the respective rule sets of these participating businesses each rule met the standard definition of that term, which is: 'A regulation or principle governing conduct or procedure within a particular area of activity' (Oxford English Dictionary). However, each also had the feature that there could be personal consequences for not following them (e.g. disciplinary action, including sometimes dismissal). This was reflective of the potentially serious consequences – to

[121] Particularly, businesses in the private sector.
[122] Which are: inform and train users, and monitor, restrict and discipline user behaviour (see again sections 4.2.3 and 4.4).

businesses and to people – which can flow from someone not following a rule within the context of cyber security.

These further findings from my case studies have delivered data that evidences Meaning Finitism[123] and Rule Scepticism[124]. During my scrutiny of that further data, two main themes emerged:

- Rules, and why we have them.
- Predispositions and conventions within rule-following behaviour.

Within the second of these themes, a number of subthemes were found as well. They concern more specific forces and factors which compel or constrain people's behaviour around cyber security rules. Each of these themes and subthemes, and the evidence supporting them, will be discussed in turn. First, however, it is important to specify again the rule sets that existed within the businesses at the time of these case studies.

### 6.2 The existing rule sets

As reported previously, Business A had no formal policies on cyber security, but Businesses B and C did. These fitted the definition of 'rule sets,' in that they were collations of policies on matters concerning cyber security, and non-compliance with them could lead to sanction.

Business B's rule set consisted of policies on data protection, the internet, the intranet, email, social media, and remote working[125]. Although all but one of these policies were grouped together in one section of the Office Manual, there was little other linkage between them. Notably, this business had no formal policy/procedure for reporting risks and incidents which either threatened or breached its cyber security. However, there seemed to be a near-formal policy on it, yet unwritten. Details of this emerged during responses to one of the questions in the Diary Study,

[123] By way of reminder, Meaning Finitism insists that meaning does not *explain* use, it *comes* from use. Consequently, Finitists reject the deterministic notion that meaning is fixed within, and by, rules themselves. Instead, they argue that people generate meaning as they go along, moving from past to new instances of rule application, and that 'correct' use of a rule is determined by normative standards set and maintained by consensus within the social collective of interacting rule-followers.
[124] By way of reminder, Rule Scepticism looks beneath and beyond rule-following practice to identify other sources of influence upon it. These include psychological dispositions, communal consensus and social conventions.
[125] Redacted copies of all these policies can be found in Appendix A on page 155.

and then also in the follow-up Interviewing. This 'policy' originated from verbal and email communications between the IT Manager and other members of staff, and had since been maintained by word of mouth[126].

Business C's rule set consisted of policies on data protection, the use of its IT systems, email, social media, and remote working. These were situated in three separate documents[127]. Although this business also had no formal policy/procedure for reporting risks and incidents which either threatened or breached its cyber security, again there appeared to be a near-formal policy on it, details of which emerged during the Diary Study and the follow-up interviewing. Several of the participants, including the Chief Executive, made mention of a 'policy' of reporting any such things to the Office Manager. This was originated, and then maintained, by word of mouth[128].

### 6.3 Rules, and why we have them

Altogether, the data presented in this chapter will identify the importance of Meaning Finitism and Rule Scepticism for cyber security. To begin with, some of those data provide insight of how people view the concept of 'rules,' and why we have them. It is interesting to note first the opinions of some people at or near the top of the three businesses. These are the people who make or assemble the cyber security rules that all employees are *expected* to follow. The tension surrounding these matters is detectable in their comments.

Rule-following – or the lack of it as envisioned by the rule-makers – seemed to be an ongoing source of frustration for the Chief Executive of Business C, who said:

> 'I have to regularly remind people – and not just internally, but the other organisations that we support – that if you've got a policy on something, it's there for a reason, and actually the worst thing you can do if you've got a policy is to ignore it' (P4/C/Int).

[126] I will explore the matter of informal collective practices in the absence of rules in greater detail towards the end of this chapter.
[127] Two of these policies (data protection and use of IT systems) were in one document, two more (email and remote working) were in another document, and one (social media) was in a third document. Redacted copies of all these policies can be found in Appendices B (page 166), C (page 171) and D (page 175).
[128] See again note 126.

These comments could be seen to imply that, when people *do not* ignore rules, the resulting behaviour will usually match that which the rule-maker is calling for (i.e. that it will be unproblematic).

In Business A, there was a lack of formal policy on cyber security, but the owner recognised the need to address this and was planning to create a 'cyber security policy.' Indeed, he had agreed to participate in the case study because he thought it would help him determine both the scope and the content of that policy. Looking ahead to it, his view on rule-following was similar to that just mentioned, because he thought of it in terms of simple adherence to rules: 'Everybody has got a responsibility for following what the policy says' (P1/A/Int). The implication here is that rule-following is simply a matter of doing what you are told, of towing the (clearly-drawn) line. Indeed, he planned also to create (legal) rules concerning adherence to those (cyber security) rules:

> 'It might also be wise to put something in their contract of employment, some specific terms relating to cyber security and their responsibilities; it makes it explicit' (P1/A/Int).

In Business C, the Office Manager complained that:

> 'It's quite hard sometimes to get everybody to do stuff. You know, you pass on the information to staff, but whether they are doing it in reality….It's hard. You feel like you need to assume that staff can follow instructions. But whether they are actually doing it in practice…Maybe there needs to be some sort of auditing every so often of whether they are doing it' (P10/C/Int).

Here, there *is* recognition that rule-following is *problematic*, but such comments represent a particular view on *why* this is so. In essence, that view is that the rules are there to follow, but the problem is that – sometimes, at least – people *just decide* not to follow them.

The matter of people deciding not to engage with rules was mentioned also by one of the Directors of Business B. In that business there was quite a lot of policy concerning cyber security, and the main way in which it was disseminated to staff was by email. When asked whether there was a risk that employees might not read those policy emails, or just skim read them, this Director replied:

> 'Probably, yes. But, I mean, when you've got about 50 people it's difficult to know how else to do it. I mean, we have in the past sent round a memo, and everybody signs it off once they've seen it. But there's also a tendency for people just to sign it and hand it on to the next person, anyway. So, it is a bit difficult' (P15/B/Int).

Here, they were suggesting that, whichever means was used (email or signed memo), a danger of non-engagement lurked, and that it lay in people's *own* choice rather than the chosen process.

At times, the comments of these people at or near the top of these three businesses suggest they may share a similar mindset on rule-following: one that views it as predictable and straightforward, as a 'simple, impenetrable matter of fact' (Bloor, 1997). Even if they do not, sometimes their individual comments suggest a reliance upon one or more of the following three assumptions:

- That, usually, the ways to follow rules are clear;
- and those ways are marked out (pre-determined) by the language of the rules themselves;
- but often, people just choose either not to engage with rules or not to follow them in the required way.

Empirically and conceptually, these assumptions require further scrutiny, and invite challenge.

### 6.3.1 Questioning those three assumptions

First, it is important to place any questioning of those assumptions within the wider context of the two main approaches to viewing human behaviour: Individualism refers to aggregates of separate individuals and individual actions, while Collectivism speaks to unitary collective entities (Barnes, 2001).

To begin with, a central thread can be seen running through all three of the assumptions: they are linked by Meaning Determinism. This approach claims to explain the ways in which people determine the particular rights and wrongs of rule-following activity. It argues that rule-following is made possible by our ability to grasp the meaning of the concepts used in a rule, which then determines our behaviour; and that this grasping of a concept is a purely individual achievement: 'It is an individual

mental act or it is nothing' (Bloor, 1997, p.4). In other words, correct rule-following results from one's *own* correct interpretation of the *meaning* which lies within the language used to express the rule. So, translation of the language delivers the meaning, which then enables (unproblematic) rule-following. From this, it can be seen that Meaning Determinism is a key ingredient of Individualism: without it, 'the individualist would have no account of normativity' (Bloor, 1997, p.5).

Instead, rules and rule-following can be viewed with a *collectivist* eye, and I agree with those who argue that Wittgenstein looked upon those matters in this way (McDowell, 1984; Bloor, 1997). I also share the view that Wittgenstein recognised that true understanding of rule-following comes from looking at what is called a 'rule' in all its complexity and richness (Bloor, 1997).

The first two assumptions – that the ways to follow rules are marked out clearly by the language of the rules themselves – weaken under such scrutiny. Take, for example, this rule that featured in Business B's rule set: 'Employees must not compromise the security of Business B or its clients'[129]. If we take this statement seriously, the term 'compromise' might come to be applied to any number of instances. Given this, the provision of examples within the rule itself would have helped people to understand what is meant by that term. However, even if this rule had supplied such examples (which it did not), necessarily those could not have been comprehensive. For instance, would the term 'compromise' relate only to the situations specified in the examples, or to broader scenarios as well? Such questions help to challenge the common belief that a straightforward relationship exists between the text of a rule and correct adherence to it. Instead, my case studies have shown that rule-following should be viewed against the background of Meaning Finitism, which wields far greater explanatory power on this matter. It holds that the terms used in rules do not have inherent meanings, and that any such terms have been used only so many times. So, there can be no definitive list of their 'correct' application. Instead, the terms are *given* meaning each time they are *used*. In short, meaning is use (Wittgenstein, 1967).

So, there is always a 'next step' to be taken (Wittgenstein, 1978), an extension of an existing meaning, an application of a term to another situation. This is illustrated

[129] It formed part of Business B's *Use of Internet, Intranet, Email Access and Social Media Policy*. See point 1(h) of that policy, in Appendix A on page 158.

further by two rules that featured in Business C's rule set, which were: 'Don't open any suspicious attachments' and 'Don't click on suspicious links'[130]. So when, during the course of a working day[131], an employee of Business C looks at one of their many emails and wonders whether the file attached to it is 'suspicious,' it is *they* who then seemingly decide whether it is. They take the next step in the application of *that* term within *that* rule. This will involve a judgement about how similar this email is to 'suspicious emails' which they have already encountered, or been told about (for instance, by examples given within the rule itself, or in a training session, or by work colleagues, etc.). However, the key point here is that such 'decisions' cannot always be determined by the rule alone, and that in reality other factors and forces will be influencing what they decide to do – a point which will be explored in detail later on in this chapter.

Such influences from beyond or outside a rule could be more likely, and more potent, for a number of reasons. In these given examples, two such reasons lie within the rules themselves. Firstly that, without more, the term 'suspicious' is inherently subjective, and usually if someone's suspicion is not aroused they will not *consider* whether something *is* suspicious to them, or would be to others. And secondly, that the rules themselves give the employees little assistance in this matter by way of examples. They only tell them that: 'If an email is marked 'Internal,' it won't be,' and that 'if an email in your junk box looks like it's from a member of staff, it won't be'[132]. Certainly, a longer and more varied list of examples might help the employees in their classification, and might promise their employers more (remote) control over those 'decisions.' But even then, we know that the list's worth would still be limited by its *finitude*, creating the inevitable need to draw analogies between those exemplars and new cases.

However influenced, if the employee does classify it as a 'suspicious email,' they will have decided that it is an email to which that rule applies. Next, come further 'decisions' on rule-following: whether to apply the rule, and if so, how? Again, these will be subject to influences beyond/outside the rule. Also, the classification itself may

[130] They both formed part of Business C's policy on 'Dealing with spam emails' within its 'Notes on how to use Business C's IT system' document. See page 177 within Appendix D.
[131] Which could, of course, include working remotely from the office (e.g. at home in the evening, or during travel to and from the office).
[132] See again note 130.

well trigger other rules, such as whom to tell about the suspicious email, and what to do with the email itself. In turn, other factors and forces may influence these rule-following 'decisions' as well.

All of this shows us that the first two assumptions are fundamentally flawed. Rules *cannot* guarantee their own future application, and the ways in which that is done. It is *people* who determine that, *each time* that they apply them, in the *way* that they *do*. Those moments of apparent choice, and the true influences upon them, will be focussed upon in the rest of this chapter. First, however, the third assumption must also be scrutinised.

In the previous section (6.3), the senior management thinking on rule-following that I reported included comments about employees' responsibility to follow what the policy says, the need to assume that people can follow instructions, the problem of employees ignoring policy, and people's tendency to disengage from policy. A strong current of the third assumption flows through these thoughts, in that each and all of them infer that people often *choose* either not to engage with policy rules or not to follow them in the required way; and the assumption that they *choose* either of these paths allows further inferences about *why* they have done so: perhaps, because they are lazy or selfish? Indeed, such accusations continue to be made (by some) within the information security and cyber security communities today. However, this third assumption, and these types of judgements that it can bring, also need to be challenged. Not least, because they often stem from a misguided view of rule-following which looks upon it, and choices within it, in very binary terms: follow the rule, or decide not to. For example, as one of the Directors in Business B saw it: 'Generally, the mindset is that if you've got a set of rules that you have to follow, then you just follow them' [P15/B/Int]. However, rule-following behaviour is not as simple and linear as this. Wittgenstein told us how and why[133] (Wittgenstein, 1967).

To end this section, it is worth reporting that these assumptions did not feature in *all* senior management thinking. There was one exception. In Business B (the law firm), the views of two of the Directors[134] differed significantly. One explained that:

[133] See again section 2.7, and see also section 6.4 below.
[134] Business B has a total of five Directors. Three of them took part in the case study.

> 'Cyber security is a big part of compliance now. That's one of the sections that [the Solicitors' Regulation Authority] are looking at. So, you know, we have to make sure that we have policies, and we have to make sure that everybody sticks to them. So, we have no choice really' (P15/B/Int).

In stark contrast, the other Director expressed little faith in the *efficacy* of cyber security rules, and took a very restrictive view of their *purpose*:

> 'The trouble is, you get the impression that [cybercrime] is an ever-moving field of crime. And just having a policy in place might protect us in a certain way if we were sued by somebody else, but it might not actually work. Because that's what policies are for, generally. In employment, you have your staff handbook. It's helpful to the staff, but mainly the policies are there to protect you [as the employer]…I think there is a danger of having a policy and it just remaining in an office manual' (P25/B/Int).

The main difference in these two views is the degree of importance that they grant to policy rules. However, it is submitted that, *in themselves*, rules are *not* important. Alone, they lack agency and influence (Wittgenstein, 1967; Bloor, 1997). In the remainder of this chapter, I will present findings that demonstrate this lack of agency, and which reveal the reality of rule-following behaviour within these three small businesses. Specifically, they will show the true sources of influence upon employees' behaviour around cyber security rules. The comments of one employee within Business B provide a fitting start to this, capturing as they do (unconsciously) some of the essence of Wittgenstein's thoughts on rule-following:

> 'I mean, everywhere has got formal policies for everything. So, a formal policy is one thing, but that's not necessarily what makes the difference. It is the practice' (P16/B/Int).

### 6.4 Predispositions and conventions within rule-following behaviour

If meaning comes, not from the rules, but from our *use* of them as we go along (Wittgenstein, 1967), what determines how far, and in what direction, we take those rules when 'following' them? A common mistake is to think that, by insisting that meaning comes from use, Finitism sees no restraints on rule application. But it does, by recognising that each time local circumstances impinge upon us, constraining what

we do (Bloor, 1997). The most important of these is the people around us. Collectively, they impose social restraint on our rule-following behaviour, through setting and maintaining normative standards by which that behaviour is judged. Consequently, it is the *community* who determine whether someone's application of a rule is 'correct' or 'incorrect.' In this way, 'meaning is not an individual whim, but the product of coordinated social activity' (Schyfter, 2016, p.315).

The data collected during my case studies included much evidence of forces such as these exerting influence on people's behaviour around cyber security rules.

### 6.4.1 Personal traits and tendencies

Each of us has personal traits. To us, they seem like natural tendencies that come from within. During the case studies, some of the participants made mention of such personal traits and tendencies, and there was evidence of their causal significance in relation to some cyber security issues and behaviours. For example, when one of the employees in Business C told me that cyber security is not something that they take much notice of on a day-to-day basis, I asked them why this was, and they replied:

> 'I think it depends upon the type of personality that you've got. I try to get on with my day-to-day job. So, I'm quite operational, I think. More operational than strategic. I don't like reading loads of stuff. I just like getting things done' (P7/C/Int).

Clearly, this person has a firm view of what they are like, and how best they work. To them, their particular focus on doing their own job in their own way comes from them being more a 'doer' than a 'thinker,' and cyber security does not naturally feature within their focus. Necessarily, these things could shape their behaviour around cyber security policy rules. Indeed, they also commented:

> 'I think with something like cyber security, it's something that is completely different to my job, and I think it's not something that I spend much time thinking about, because it's not going to improve my performance on a day-to-day basis' (P7/C/Int) [135].

[135] Note also that these comments of this employee, and their next ones (at the start of section 6.4.2), are consistent with my analysis in Chapter 5 concerning 'friction,' policy and everyday work. See again section 5.5.3.

This mindset shows that some people look upon cyber security, not as pervasively relevant, but as something either separate or distant from their *own* working life.

Here also, there was mention of job performance. This was something that one of the employees in Business B spoke about a lot. She explained how her career ambitions necessitate her working long and hard:

> 'At the moment, while I am training, I need to be showing that I am valuable, and that I can take on as much as I can. And yes, there is quite a lot of pressure. But I think it all depends upon how much you want to put into it. There are some people who do 9am to 5-30pm, and stop there. For me though, this is meant to be a career rather than a job. So, it does overlap with your personal life, if you've got certain goals that you want to achieve' (P12/B/Int).

This increased work ethic brings longer hours of work, doing a greater number of tasks, and some of that time is spent working remotely at home in the evenings and at weekends. All of this can increase any yearning to 'get things done.' Also, a likely corollary of all that extra effort will be frequent tiredness. Busy and tired people can make mistakes, or look for shortcuts, which can undermine cyber security and the policy rules on it.

### 6.4.2 Personal interest, or lack of interest

When at work, instinctively some people have little interest either in rules or cyber security. For example, an employee in Business C confessed:

> 'I must admit that I do not spend much time reading policies. When I started the job, I spent my time reading about things I will be doing in my job, so I may have glazed over something about cyber security, but would not be sure as it is not something that would interest me' (P7/C/DS).

However, when I asked this same person whether she thought that her *colleagues* would welcome more formal guidance on cyber security, she predicted that they probably would (and, in fact, most of them did). However, she alone shows that

people's attitudes towards cyber security rules can be very different[136], and this brings both general (threat) and specific (training) implications to cyber security within any organisation.

It is not only lack of interest that brings vulnerability. Personal interest can do so as well. For example, when I was discussing cyber security risks with another employee in Business C, she admitted:

> 'It would be dead easy to get me, because I do a lot around certain information, all over my *Facebook* page, because I share a lot of information because I've got a big *Facebook* page. So, it would take very little for somebody to know what my interests are. And if they then copied one of the names that I'd been following, I'd open it [an email]….Anybody sending me an email around funding or women's issues, straight off I'd open it' (P11/C/Int).

Acknowledging that her keen interest in certain topics might interfere with her judgement on risk, she knew that this could be used successfully as bait during phishing attacks upon her. In short, that curiosity could displace caution. It is also worth noting that, when asked, this person was not sure whether the business for which she worked had a policy on the use of social media (which it did), a policy on the use of email (which it did), a remote working policy (which it did), and a policy on reporting risks and incidents that either threaten or breach cyber security (which it did not). This also supported her admission that she did not give much thought to cyber security, either in her personal or working life (P11/C/DS). Necessarily, all of this made her and the business for which she worked more vulnerable to cyber attack.

### 6.4.3 Personal perspectives on technology and cyber security

As individuals, our own attitudes towards certain things can stem from instinct, experience or a combination of both. The case studies unearthed some interesting personal perspectives on technology and cyber security, and perspectives can contribute to the shaping of practice.

[136] And it is worth remembering here that it takes only one momentary action, by one person, to undermine cyber security.

Some people seem instinctively wary of technology. As one employee in Business B put it: 'I am tech-mistrustful' (P17/B/DS). Indeed, someone in Business C admitted:

> 'I am very nervy about computers. I love them, but I am very nervy about them, because I think that we are ignorant to the power that they have, or how people can [mis]use them' (P11/C/Int).

Other people can feel very uneasy on the subject of cyber security. For example, as already mentioned, one Business B employee revealed that: 'At the moment, I find the whole thing [cyber security] quite daunting. And you can become quite overwhelmed by it, and quite scared by it' (P29/B/Int). It seems that similar tensions can be felt by senior managers as well. Another Business B employee reported that: 'The IT Manager is a man on a mission with it [cyber security). And we have Directors who are apoplectic with fear' (P16/B/Int).

Several participants linked their own *experience* with technology and cyber security to the shaping of their perspectives. For example, when talking about the challenges of understanding and responding to the many cyber security updates sent out by the Law Society, one person in Business B said: 'I think that if you have a non-technical background, it's difficult to actually think technical' (P28/B/Int). Indeed, some participants felt that their own experience truly differentiated them from their colleagues, making them less of a cyber security risk than those other people. For example, one said:

> 'I like to think I'm probably a bit more switched on, because I've got a bit of a background in IT sales….So, I like to think that I'm quite alert to it. Whereas, I would think that quite a lot of my colleagues aren't quite up to the same level. [Although,] I could easily still be tricked. But I just think that there are probably colleagues who are a bit more naïve than I would be' (P21/B/Int).

It was not only naivety that was cited as a possible weakness. Potential lack of care was also linked to lack of experience or expertise. For example, when being asked about cyber insurance, an employee in Business B commented:

> 'I'd like to think that in the Accounts Department we are probably more aware of the threat than a lot of other people in the firm. But I think that there are some other people in the firm who, if they knew that we were insured, might

> be more blasé about it, perhaps thinking: 'Oh it's ok, now we're insured'…But we are in Accounts, so we would always be on the lookout for cybercrime' (P20/B/Int).

However, here it must be reported that people's own perspectives on this particular matter varied significantly. Certainly, some thought that if the business took up cyber insurance this might make them less vigilant[137]. For example, one person replied:

> 'Yes, it sounds awful, but I think I would be less worried. Because we've talked about all of these serious consequences, it makes you much more wary, knowing about them. But if you've got that mental security blanket of: 'If it all goes pear-shaped, it's fine.' Which is silly, because it would still happen, you'd still go through all those processes and all that stress, and your money going or your reputation. But you would have that sort of mental security blanket' (P6/C/Int).

However, many people thought they would remain just as vigilant[138], and some even more so. For example, one person said:

> 'I think it would make people feel a lot more vulnerable, because rather than it being a possibility, as soon as you get insurance for something it is almost like you're accepting that, whilst it's not inevitable, it is a higher possibility than it would be if you didn't have insurance, if that makes sense? So, I think it would make everyone a bit more switched on, a bit more alert' (P23/B/Int).

However, a different form of complacency *was* detected in some people's perspectives on cyber security *in general*. This surfaced when I was asking each of the participants how much thought they give to cyber security in their working life. Some people reported thinking about it only a bit[139], quite a lot[140], or a lot[141] when at work. However, the comments of some others revealed a particular mindset on cyber security, and on who bears responsibility for it within the workplace. For example, one person in Business B said: 'I think about it [cyber security], but rely on the fact that we employ a full-time IT Manager to take care of this' (P25/B/DS). Similar

[137] P6, P9, and P10/C/Int; P24/B/Int.
[138] P5, P7 and P8/C/Int; P12, P13, P14, P15, P16, P18, P19, P20, P22, P26, P27, P28 and P29/B/Int.
[139] P5, P6, P9, P10 and P11/C/DS; P11, P12, P13, P16, P17, P22 and P25/B/DS.
[140] P4, P7 and P8/C/DS; P14, P15 and P29/B/DS.
[141] P19, P26, P27 and P28/B/DS.

attitudes can also occur where people from outside the business provide the IT Support, etc. Indeed, the Chief Executive of Business C recognised this: 'Possibly the biggest risk for this organisation is that sort of complacent feeling that we pay an external body to do this [IT Support] for us' (P4/C/Int).

Perhaps the most striking example of such complacency[142] came from an employee in Business B, who said: 'I assume that when I am at work that cyber security is already being dealt with by various different softwares that are installed' (P24/B/DS). Clearly, such perspectives can undermine cyber security. In particular, people who have this mindset are much less likely to engage with, let alone follow, any existing cyber security policy rules. Here, some might be tempted to think that there are other reasons behind those people's decision not to engage with those rules (e.g. laziness or selfishness), but that quick assumption should be resisted. Instead, their own words suggest simply that, for whatever reasons, they do not yet appreciate the responsibility placed upon them by their employers, and their role in maintaining the cyber security of the business. Also, it is interesting to note that neither age nor job level connected these people; nor, therefore, their misunderstanding. The first of them (P25/B) is 65 years old, and is one of the Directors of the law firm. The other (P24/B) is 22 years old, and works as a Litigation Assistant[143] within the firm. Whatever the direct sources of their misunderstanding may be, other factors might be sustaining it as well. For example, either of those two people may have a similar mindset to that employee in Business C[144] who 'just likes getting things done,' and views cyber security as 'something that is completely different' to their job (P7/C/Int).

### 6.4.4 Professional experience and job status/level

One participant suggested that working for the same organisation for a long time might stifle experience in cyber security and cloud perspective on it. He explained:

> 'There are cyber security habits that I have brought from every job that I've had since I was eighteen, which are not always present in people who have

[142] There were others as well. For example, an employee in Business B admitted that they think less about cyber security at work than in their personal life 'as safeguards are already in place' (P21/B/DS).
[143] A comparatively low-level job (mostly involving typing), and done in a different department from the one which P25 runs.
[144] See again the comments of P7/C/Int within section 6.4.1.

been here for 30 years or so. And I think that's a matter of vulnerability' (P16/B/Int).

The key point here is that, beyond the signposts of training, when he and someone else are asked to justify some particular behaviour around cyber security, they will each be inclined to say: 'this is simply what I do' (Wittgenstein, 1967: 217); and what *he* does may well be different from what that other person does, *partly because* he has worked in different organisations along the way. However, of course, the 'correctness' of his actions will be determined neither by him nor the people with whom he used to work. It will be decided, through consensus, by the people with whom he *currently* works (Wittgenstein, 1967; Barnes *et al.*, 1996; Bloor, 1997), and behaviour which is deemed 'correct' may or may not also threaten cyber security. In short, correctness does not necessarily equate to secureness.

Here, it is also worth noting that age might contribute to differing action as well. This participant was aged 27, making him a 'digital native'[145], and the people with whom he was comparing himself were in their mid-40s or older, making them 'digital immigrants.'

It was also suggested that people's lack of professional experience can sometimes generate distorted perspectives of *them* – who they are, and what their intentions might be. For example, an employee of Business C reported that:

> 'In the charitable sector, some of the people with whom we communicate are volunteers, and the ability of some of them to word an email in a professional way is limited. So, sometimes their emails can be wrongly thought to be spam because of the unprofessional wording within them' (P6/C/Int).

If a business uses a spam filter, such emails will be diverted away from other employees[146], bringing a certain set of problems. But if it does not use one, or if the filter is set rather low, those employees will receive the emails, bringing a different set of problems; namely, confusion and tension around cyber security.

[145] The world wide web was first delivered over the internet in 1994, when the first commercial web browser (Mosaic) arrived. So, this individual would have been born into the 'Internet Age,' and would have grown up with digital technology ever-present in his life. However, note also the claim that the term 'digital native' is neither empirically nor theoretically informed, and so may simply be a sweeping generalization (Bennett *et al.*, 2008).

[146] At first glance, these may look like mistakes made by code (spam filter), but the code is set by humans (spam filter levels are adjustable), so these are human decisions.

The issue of job *status* was also mentioned as a possible cause of cyber insecurity. In Business B, a senior manager commented:

> 'I think that the number of high level part-time workers that we have creates an air of vulnerability. If someone wanted to target us, it would be very easy for them to say: 'Oh, I spoke to X.' And if X is gone for the rest of the week, and it's Wednesday lunchtime and they are speaking to Y, then that gives credibility from X, which could enable them to get in' (P16/B/Int).

This was an interesting observation on how a business with a mixed workforce (full-time and part-time) might be more vulnerable to attacks involving certain social engineering techniques. It is also particularly relevant as we enter the age of flexible working, in which at least 40% of employees in the UK would like to work flexibly[147] (Peacock, 2014), and in which all UK employees have now been given the legal right to request flexible working hours (Milne, 2014). Alongside reduced or different hours of work, and job sharing, the definition of 'flexible working' can include *remote working* – more on which later.

Also, some people may mistakenly perceive that their job *level* exempts them somewhat from responsibility for cyber security. For example, when I was asking one of the Business B employees about their own degree of vigilance towards cybercrime while at work, and whether the uptake of cyber insurance might affect this, they replied:

> 'I kind of think that as an employee – I know that it might sound really bad – that this is the kind of thing that you wouldn't necessarily think about. I'm just a normal employee[148], whereas Directors might think like that' (P24/B/Int).

Again here, one can detect that mindset of just wanting to 'get on with your job' and 'get things done.'

### 6.4.5 Workload and worktime pressure

Necessarily, that same mindset or predisposition can also be influenced by a person's own workload – by the amount of things that they 'just want to get done.' Also, of

[147] In this particular survey, 'working flexibly' was defined as either working part-time or working from home.
[148] This person is a Legal Assistant in the firm, which is a lower level job that mostly involves typing.

course, an individual's workload does not normally lie within a vacuum. Other people's workloads can affect it, simply because workloads fluctuate. For example, an increase in the workload of a colleague (e.g. a manager) may bring more work to you, or the temporary absence of a colleague could do the same. In turn, might that influence *whether* – in an instant, or for a longer period of time – you follow a cyber security policy rule, or *how* you follow it?

Certainly, I found evidence within these three businesses that workloads, and their fluctuation, can influence people's behaviour around cyber security in general, and policy rules in particular. First, it is worth noting that workloads can be increased, or work rates slowed, by rules imposed on a business by organisations other than itself. The most obvious example of this is new laws. For example, as a law firm, Business B will be experiencing increased demands for legal advice about post-Brexit futures, both personal and corporate. Also, some of Business B's employees made mention of the need to comply with an increasing number of rules laid down by non-government organisations, such as the Law Society and the Solicitors Regulation Authority (SRA). For example, it will be remembered that one person observed:

> 'We're already in quite a heavily regulated industry [the legal sector], and I think it puts quite a lot of people off. Because there are definitely aspects of this job where you feel like you are just doing compliance more than anything. And you kind of think that your job is just going to become compliance; that you will not actually be doing your job most of the time' (P21/B/Int).

The point here is that his latter comments suggest real concern about friction between complying with rules – relating either to cyber security or other matters – and 'just getting on with your *real* job.' Wittgenstein stressed the importance of viewing any apparently individual judgement, action or reaction against the background of 'the whole hurly-burly of human actions' (Wittgenstein, 1967a: 567). Rule Sceptics have read this as meaning that:

> 'each individual episode is understood as being part of an overall weave, with the individual threads of action appearing and disappearing like the warp and weft of a fabric' (Bloor, 1997, p.99).

One of the Directors of Business B confirmed that cyber security itself has become 'a big part' of the compliance rules laid down by the SRA; and so, she explained: 'We

have to make sure that we have policies [on it]' (P15/B/Int). I asked all of the participants whether they thought that more formal policy on cyber security might interfere with their ability to do their own job. In Business B, an interesting range of replies were given. A number of people thought that it would not interfere significantly[149]. Indeed, one of them commented: 'We always work to adapt. It's simply part of everyday life' (P28/B/Int). She seemed to view rules as inevitable threads in the working weave, but others had reservations. For example, one person stressed that:

> 'People need to know that a policy is achievable, that they actually can do it and incorporate it into their day. Whereas, if it's thrown in or launched too quickly, then it's immediately going to cause friction' (P23/B/Int).

This was interesting. The scenario they described includes the potential dangers of swift assumption and misplaced blame. In that situation and others, the friction could lead to someone not following a policy rule, or not following it in the way intended by those who made it. More specifically, either because that friction has made them 'choose' not to follow it, or made them *change the way* in which they follow it. However, this would be due to factors of increased workload and/or worktime *exerting influence* on their rule-following behaviour, and not necessarily because they did not follow the rule for other reasons, such as laziness or selfishness.

A number of people in Business B predicted that more formal policy rules might slow the *pace* of their work[150], but they did not seem too worried by this prospect. However, some other people were. One spoke of feeling increased pressure when work processes are injected with more formality (P14/B/Int), and it will be remembered that another person admitted to having 'huge concerns' about an 'over-zealous approach' to the introduction of more formal policy (P16/B/Int). Also, someone else complained that: 'It's starting to feel as if the job is more like a procedure checklist' (P29/B/Int). To some then, more rules can mean more stress; and, potentially, stress can influence judgement and practice.

The employees in Business C had fewer concerns about this. Most of them predicted that more formal policy would not really interfere either with their workload or their

[149] P13, P19, P22, P26 and P28/B/Int.
[150] P14, P15, P17, P20, P24, P25 and P27/B/Int.

work rate[151], and the few who thought it might did not seem perturbed by this[152]. However, people did emphasise the importance of keeping any new rules 'workable'[153] and writing policy that is 'practicable and useful'[154]. These appeals to pragmatism are yet more evidence of what seems to be many people's main concern in the workplace, which is 'just getting things done.'

### 6.4.6 Technological obstacles and 'workarounds'

Necessarily, technology itself can be a very direct influence on practice. Indeed, some participants revealed that technological problems were *shaping* their work choices. For example, one of the senior members of staff in Business B complained that such things had affected his willingness to work remotely. He explained:

> 'I have worked for a number of [law] firms where you actually log in on your computer remotely. Here, we've got it through an *iPad* which doesn't really work, so I've given up on it...In other firms that I've worked for, you could work from home and be looking at the actual hard drive – the server, not your own hard drive. But here we work on hard drives. It's just not the same as working from a remote server…The IT Manager said that with the *iPad* you have some kind of parallel app. But it was so rubbish, and you had to have the computer on here [in the office, simultaneously]. But I've come from a place where you let nobody know your password, you let nobody use your computer, you must never leave it on [logged in] when you are physically away from it…Here, to use the *iPad* you have to leave your computer on, which would mean that anyone here could use my terminal to access it. And I'm not comfortable with that. That could include a cleaner, or even a client wandering around' (P17/B/Int).

Here then, problems with technology have affected *what* this person does, and *where* and *when* he does it.

[151] P5, P7, P9, P10 and P11/C/Int.
[152] P4, P6 and P8/C/Int.
[153] P11/C/Int.
[154] P4/C/Int.

In such cases, another problem lurks: the temptation towards 'workarounds'[155]. Indeed, it is said to be human nature to look for them in these situations (Sasse and Flechais, 2005), and more so perhaps when someone is just wanting 'to get things done.' For example, another person in Business B admitted to doing this. They explained:

> 'Originally, I worked at home one day a week, because I lived far away. So, my home PC was set up to work from the network, so that I could work at home [via a remote desktop facility]. But since the IT Manager changed our service provider, I can't work on my PC from home. I don't know why, but he hasn't managed to sort that out. So, I have to work on my *iPad*. It is limiting. I mean, I can work on my emails, I can get into my desktop – I've got a parallel thingy [app] – but the thing that concerns me is that if I've got to do a document I have to email it to myself on my home email address, then work on it, and then email it back. Because I can't do major work on my *iPad*. It's a workaround, but it works. If I'm drafting a document, I just draft it on my PC and email it to myself. But that's an additional concern: that I've got documents flying about [in cyberspace] via my Sky.com email account, which probably isn't the best thing' (P25/B/Int).

In particular, three things are worth noting here. Firstly, that this is an example of how changes in technology from usual working practices can also change the similarity relations between past exemplars and new cases. Secondly, that this person *realises* that their workaround behaviour potentially threatens the firm's cyber security, yet they continue with it because, in their own words, 'it works' – and thereby allows *them* to work. And lastly, that their temptation towards this workaround behaviour must be strong, because they continue with it despite being a Director of the firm, with responsibilities which include writing most of its policies – one of which is the policy on remote working. That policy states that the copying of documents from the firm's computer network to personal computers (as here, via email) cannot be done

[155] The term itself is helpfully descriptive, but a more formal definition of a 'workaround' is: 'A goal-driven adaptation, improvisation or other change to one or more aspects of an existing work system in order to overcome, bypass or minimise the impact of obstacles, exceptions, anomalies, mishaps, established practices, management expectations or structural constraints that are perceived as preventing that work system or its participants from achieving a desired level of efficiency, effectiveness or other organisational or personal goals' (Alter, 2014, p.1044). See also Leigh Star (1987) and Timmermans and Berg (1997), but note that they use instead the term 'tinkering.'

without the express permission of one of the Directors, on each and every occasion[156]. Clearly, this Director continues to give *herself* such permission, but this persistent practice – done to work around a technological obstruction that continues to be left in place – undermines the policy itself and the cyber security of the business.

There was evidence also of other workaround behaviour. For example, several people cited problems with the remote desktop facility in Business C[157]. As one of them explained:

> 'When I was off sick [for 3 months], I logged in and used the remote desktop facility from home on a few days, and it was *so* slow. Frustratingly slow. I mean, not just on sending email, but even when you were using things which you wouldn't normally use the internet for, such as typing a Word document. It was painful' [P6/BC/Int].

Another person confirmed that, because of the slowness of this facility, people sometimes send documents to their personal email addresses, or put them onto a memory stick, in order to then work on them at home (P5/C/Int).

In Business B, one of the employees admitted to doing this, but for a different reason. They had never set up the remote desktop facility on their home computer – perhaps because that computer was an Apple Mac, which required an extra step in this setting up process [158]; and so, they explained:

> 'If you are just wanting to look at a couple of documents over the weekend, it is quite easy just to email it to yourself'; more specifically, easier than having 'to borrow a work laptop from the IT Manager that is all set up properly for remote working' (P12/B/Int).

Perhaps the most striking example of workaround behaviour within a remote working setting came from the owner of Business A. During a period when his own laptop was

---

[156] Business B's remote working policy is found within its *Use of Internet, Intranet, Email Access and Social Media Policy*. See specifically point 5 of that policy, in Appendix A on page 159.

[157] Business C's remote working policy permits only two ways of working remotely. The main way is via a remote desktop facility. The other way – to be used only where someone encountered problems with the main way – is via remote web access (by typing a specific URL into their web browser). These rules are found within the Business C's *Notes on how to use Business C's IT system* – respectively, within the sections entitled 'Accessing the server remotely' and 'Remote web access.' See Appendix D, pages 175 and 176.

[158] Downloading some other software first before being able to load the remote desktop facility software.

being repaired, at home he used his son's laptop to remotely access files on the business's system. During interview, when I suggested to him that using someone else's device to do this was risky, he replied: 'Yes,…[and] my son's laptop is probably especially risky because he's on *TOR* and *4chan* and all kinds of things like that' (P1/A/Int). He also admitted more risky workaround behaviour:

> 'My son's laptop is very slow, maybe because it has too little memory, but it also seemed to be running some Windows anti-malware that was eating up a lot of the computer's resources….[So] I searched a few Windows user forums to find ways to disable *Windows Defender,* which seemed to be the culprit. This improved the performance a bit' (P1/A/DS).

After pointing out to him that slow performance can sometimes be a symptom of malware infection, I asked him whether, when he disabled the anti-malware program, he had put any other protection in place of it. He confirmed that he not.

These examples, drawn from all three businesses, show that technological hitches and hurdles can be a contributory cause of insecure practice. Also, because they concern remote working, they rebut more strongly any quick assumptions about other causes of such behaviour (e.g. laziness). In most of these situations, people were working from home outside their normal working hours – in the evenings and at weekends – and it was a combination of technological problems and their concern to 'get work done' that caused them to workaround in risky ways. Again, this demonstrates how local circumstances, including personal dispositions, can influence an individual's behaviour around rules. That behaviour will be 'correct' or 'incorrect' according to the collective judgement of the people around them, and 'correct' practices can also be insecure practices.

### 6.4.7 Anticipation of formal sanctions

Law is seen as one of the four main ways of regulating human conduct[159] (Lessig, 1999). Law constrains behaviour through the punishment that it threatens. Businesses use law as a means of controlling their employees' behaviour, and these three small businesses were no exception.

[159] The other three being Social Norms, Markets and Architecture (Lessig, 1999).

In particular, the sanctions delivered by Employment Law cast their shadow over working practices. The possibility that misconduct could lead to them losing their job often shapes employees' behaviour in the way desired by their employer. But sometimes this does not happen. When, during the course of the case study, the owner of Business A dismissed one of his employees for two alleged breaches of cyber security, that employee was said (by the owner) not to understand the gravity of his misconduct – possibly, in part, because the business had no *formal* policies on cyber security[160]. However, that dismissal seemed to sharpen the mind of the remaining employee, who now thought 'that it would be prudent to have a measure of policy' on cyber security (P2/A/Int). The point here is that legal sanctions can shape behaviour either via the *threat* of their use or by the *fact* of their use (e.g. against someone else).

The rule sets of Businesses B and C each made mention of the possible sanctions for breach of their cyber security rules. For example, Business C's policy on the use of social media included this strong message:

> 'Breach of this policy may result in disciplinary action, up to and including dismissal. Disciplinary action may be taken regardless of whether the breach is committed during working hours, and regardless of whether our equipment or facilities are used for the purpose of committing the breach. Any member of staff suspected of committing a breach of this policy will be required to co-operate with our investigation, which may involve handing over relevant passwords and login details.'[161]

Within Business B's rule set there were similar messages. For example, this statement featured at the end of its *Use of the Internet, Intranet and Email Access and Social Media Policy*:

> 'If any user is found to be disregarding [this] policy, the Directors reserve the right to disconnect them immediately, and they may be subject to further action under Business B's disciplinary procedures.'[162]

---

[160] It will be remembered that the owner of Business A explained this absence of formal policy in the following way: 'We are under quite heavy financial pressure the whole of the time. So, writing a cyber security policy doesn't do well in the prioritisation wars with phoning a customer or delivering the service. So, that's why it hasn't happened. It's not that I don't think it's important. But, on the scale of things, it's one of these things that is a job that's constantly getting postponed' (P1/A/Int).

[161] Business C's *Social Media Policy*. See Appendix B, at the top of page 167.

[162] See specifically the end of point 7 of that policy, in Appendix A on page 160.

And later on within its rule set, this more general (and stronger) warning was given:

> 'Employees who breach any of the above policies will be subject to disciplinary action, up to and including termination of employment.'[163]

Even if some of the employees had not actually read these written statements, all of the participants (in all three businesses) seemed fully aware of an ever-present threat of disciplinary action for breach of policy rules, on cyber security or any other matters. Here, it is worth remembering that certain other rules – imposed on the businesses by organisations other than themselves – were also contributing to this regulatory mix. For example, it will be remembered that one of the Directors of Business B (the law firm) mentioned that cyber security is a 'big part' of the compliance rules laid down by the Law Society (P15/B/Int); and Business C (the charity) is subject to regulation by the Charity Commission, which now recognises cyber security as a key issue for charities today[164]. It is also important to note that breaches of certain rules laid down by these regulatory organisations must be reported back to them, with the possibility of further action being taken. For example, during the case study I was told that Business C had recently reported to the Charity Commission a case of attempted fraud, perpetrated via a spear phishing email sent to Business C's Finance Officer[165]. There are also rules which businesses themselves adopt voluntarily. For example, Business C uses the ISO 9001 set of management standards[166]. Therein, for example, the non-conformance reporting procedure is used to report/record incidents that either threaten or breach the business's cyber security[167].

For these businesses, gaining insurance can seldom be viewed as 'voluntary.' For instance, as a law firm Business B is required to have Professional Indemnity

---

[163] See specifically the end of the section entitled 'Personnel responsible for implementing this policy,' in Appendix A on page 161.

[164] See, for example, the section on Cyber Security within one of the Charity Commission's recent guidance documents, entitled: 'Making Digital Work: 12 questions for Trustees to consider' (Charity Commission, 2016).

[165] A spear phishing email is one that targets a specific person. Usually, such an email purports to be from someone whom the recipient knows and trusts. In this case, the email purported to be from Business C's Chief Executive, asking the Finance Director to make a swift payment of several thousand pounds to another company's bank account. Luckily, the Finance Director telephoned the Chief Executive (who was at an event in another part of the country) to confirm this with her before making any payment. They then reported this matter to the police, and soon after also reported it to the Charity Commission.

[166] This is a set of (certifiable) standards for a quality management system, laid down by the International Organization for Standardization (ISO). See further at https://www.iso.org/iso-9001-quality-management.html

[167] These non-conformance reports are sent to, and then reviewed by, Business C's senior management.

Insurance[168]. But during the case studies I questioned all of the participants about cyber insurance[169]. One of the questions that I asked each of them was: If this business decided to insure itself against cyber security risks, do you think that would affect you in any way? To this, I received an interesting range of replies. Some people felt that, indirectly, this might *lessen* the business's control of their behaviour around cyber security. Specifically, because it might make them somewhat complacent and less vigilant[170]. For example, one person in Business C admitted:

> 'I'd be a little less cautious, which wouldn't be a good thing, necessarily. If we were insured, then I might risk it sometimes, if I thought that checking it further would make things awkward and hold things up' (P9/C/Int).

Again here, the desire or pressure to 'get things done' is a detectable influence upon behaviour around cyber security. Somewhat surprisingly, an employee in Business B seemed to think that such insurance cover might give more protection – to them as an individual employee and to the business – than in fact it would or could. She spoke of this when citing the example of receiving a phishing email:

> 'I guess [cyber insurance] would give more of a safety net, if you did do something. I guess that – I don't want to say you wouldn't worry as much about it – but you would probably be more inclined maybe to click on that link [within what turns out to be a phishing email]. I mean, if you know that it will be fine because we've got insurance, you might be intrigued to see if it is, or not [what it appears to be]' (P24/B/Int).

However, it is also important to note that a number of the participants thought instead that the take up of cyber insurance would likely *increase* the business's control of their own cyber security behaviour. For example, several of them recognised that the conditions of any such insurance could well add to the number of rules on cyber security that employees were expected to follow. As one person in Business C put it:

---

[168] See the Solicitors Regulation Authority's Indemnity Insurance Rules 2013. Available from http://www.sra.org.uk/solicitors/handbook/indemnityins/content.page

[169] At that time, none of the three businesses had taken up cyber insurance, but Business B was planning to do so, and the Chief Executive of Business C told me that she was considering this option.

[170] P6, P9 and P10/C/Int; P19 and P24/B/Int.

> 'Well, insurance has always got conditions to it, hasn't it? So, there would be things that we must or must not do, in order not to jeopardise the insurance coverage' (P5/C/Int).

Another person shared this opinion, saying:

> 'If you weren't to invalidate your insurance you would have to comply with a whole new set of standards that the governance of that insurance would demand to be in place; otherwise, the insurance would be invalid' (P8/C/Int).

Indeed, one of Business B's Directors commented:

> 'I would hope that people wouldn't just think: 'Oh well, they've got the insurance, so it doesn't matter' – because an insurance company will try to find any reason not to pay out' (P13/B/Int).

As another person in Business B put this: 'The insurance company would no doubt word the agreement in a way that they could still investigate whether you were to blame or not' (P14/B/Int) – and that would likely also involve the investigation of which individual employees were at fault (e.g. by not obeying a policy rule on cyber security).

Clearly then, the anticipation of formal sanctions is another of the contingencies surrounding rule-following practice, and holding potential influence over it. But also, a business's own set of cyber security rules (and related official sanctions) must themselves be viewed in the light of any other rules that could influence them, such as rules laid down by governing bodies (e.g. the Law Society or the Charity Commission).

### 6.4.8 Being busy, serving immediate purposes and pragmatism

As reported in the previous chapter, the majority of the participants in these case studies (23 out of 28 people) welcomed the prospect of a greater amount of formal policy on cyber security within the businesses for which they work[171]. So, most of them are not averse to more rules on this matter. Indeed, to some of those people the prospect of no further rules seemed unwelcome. As one Business B employee put it:

[171] See again section 5.3.

> 'Yes. The more the better, basically. I think it just needs to be drilled into everybody that [cybercrime] is a serious threat. And people need to always have it in the back of their minds, throughout the working day. And not think: 'Oh well, I'm not going to be targeted.' Because they might be' (P20/B/Int).

Another person mentioned that 'there is a bit of a fear of the unknown,' and stressed the need for everybody to know 'exactly what to do' if they encounter a cyber security threat (19/B/Int). Others commented that having such rules is 'really important' (P23/B/Int) and that 'policy like that would always help' (P22/B/Int) because 'everybody appreciates having a set of rules' on such things (P15/B/Int).

However, one person's comments on this matter struck me more than these others. They said: 'I think it's important to have those procedures and policies in place. At the end of the day, *everyone wants to follow the procedures* [my emphasis]' (P23/B/Int). This may be the case, but likely is not. Given the evidence just provided that 5 out of the 28 participants would not welcome more rules on cyber security, it is probable that at least 1 of those 5 people does not welcome *any* such rules (existing or proposed), and so seldom wants to follow them. Indeed, one of the Managers in Business B predicted as much:

> 'I imagine there are a few people here who would rather just have their head in the sand, and I don't think they'd welcome formal guidance on anything, let alone cyber security' (16/B/Int).

However, the important point here is that so far in this chapter I have provided evidence of a number of factors which can, and do, influence rule-following behaviour, and that many of these factors neither involve, nor link to, people simply choosing not to follow the rules *just because* they don't want to (for example, because they don't care about the business's cyber security, and/or because they can't be bothered to follow any rules on it). This also remains true for the factors that I will discuss next.

For many of the participants, busyness featured strongly in their working lives, and often their busyness led to friction with cyber security rules, a frequent consequence of which was that in a busy instant they 'decided' not to follow one or more of them. Here, it is worth remembering how much rule-following behaviour can be influenced

by the attempted communication and embedding of the rules themselves[172]. On this matter, a number of the participants alluded to busyness being a reason behind their lack of engagement with rules[173], and some cited it specifically as the main reason for such behaviour. For example, one of the Business B employees admitted:

> 'Even though we receive emails [from the IT Manager], when people are having a busy day at work it is easy to open an email, read it once, think 'I've read that, that's done,' and then just delete it, or skim read it, and not take everything in properly' (P23/B/Int).

Another person explained:

> 'When the IT Manager sends round an email about it [cyber security], you sit there and you have a few minutes panic about it. But then we are so busy that that feeling doesn't last all day. You read something, and it makes you think about it. But actually, by the time you've picked up the next file [task] it's almost gone' (P12/B/Int).

Someone else told me that the IT Manager sent out such emails 'maybe once or twice a day,' but that 'a lot of people choose not to read them'; and anyway, that same person thought it 'very easy just to skim past an email, delete it, and then tell someone that you've read it' (P24/B/Int). Indeed, the person who writes most of the policy documents in Business B conceded that:

> 'If you just send someone a policy [via email],…they will just ignore it. In fact, quite often they would probably just delete it, without doing anything. I do it myself' (P25/B/Int).

Next, a certain irony must be noted: that by giving people who claim already to be busy more behavioural rules, you risk making them even more busy, because there is a real danger that additional rules *themselves* could increase time pressure on existing workloads. Several of the participants made mention of this when I asked them whether they felt that their ability to do their job is hindered by cyber security considerations, rules or practices. One Business B employee reported that: 'At the moment, we are being given a lot of new procedures to follow' (P29/B/DS). Another

[172] See again section 5.4.3.
[173] P8 and P9/C/Int; P12, P17, P20, P21, P23, P24, P26, P27/B/Int.

person explained that cyber security considerations and rules have brought extra procedural steps, 'because you need to check third parties all the time' (P15/B/Int). Two other employees confirmed this, saying that 'many more checks have to be done' (P13/B/DS) which 'is time-consuming, and therefore prevents us doing something else' (P29/B/DS). Here again, one can sense the tension between following cyber security rules and 'just wanting to get (other) things done.'

Two more examples provide further evidence of that tension, and the first of them brings another ironic twist. As mentioned in the previous section, Business C uses the ISO 9001 set of management standards[174], which include the non-conformance reporting procedure that is used to report/record incidents that either threaten or breach the business's cyber security. However, the person who is responsible for writing such Reports admitted to me that she is usually too busy to do this when it is meant to be done:

> 'We have this ISO 9001, under which we are supposed to report things that have gone wrong, or incidences and that sort of thing. And I only generally think to report things to that at about 3am, two days later. Normally I then do, but it's not always my next port of call' (P6/C/Int).

Her comments suggest that, usually, busyness prevents her from reporting (or thinking to report) incidents in a timely manner[175], and also that busyness then shapes her *own* scheduling of when she will do this. In short, more immediate purposes will often take priority.

The second example also features this. But, more alarmingly, in direct response to some potential threats themselves. The Finance Officer within Business C admitted to me:

> 'I don't ever know whether to click on certain things that come into my junk email box...Whether it's safe or not. *Sometimes I risk it. I don't want to miss anything* [my emphasis]' (P9/C/Int).

[174] See again note 166 and 167.
[175] And here it is submitted that, when it comes to reporting cyber security threats and incidents, time is of the essence.

In this way, her concern not to endanger the cyber security of the business seems regularly to be overridden by her *greater* concern to be aware of *all* significant matters (i.e to know all the things to get done). Also, pragmatic arrangements in pursuit of 'getting things done' can sometimes really increase such risks. For example, one of the Directors of Business B told me:

> 'My emails are copied to my secretary. And she opens my emails. And even the ones that are not copied are often accessible by others. For example, I have access to the email boxes of all the people in my department, and they have access to mine. So, somebody else could open an email. So, we all need to be vigilant' (P25/B/Int).

Clearly also, pragmatism drove the workaround activity that was discovered in relation to rules on remote working[176]. Those who did it chose pragmatically to sidestep technological hurdles on the way to 'getting things done.' But some others did the same with a somewhat different state of mind. For example, Business B's remote working policy states:

> 'You are not allowed to copy documents from the Company's computer network on to personal memory sticks or personal computers without the express consent of a Director on each and every occasion…Those Directors, Managers and Fee Earners *authorised to work periodically from home*, should already have been given a direct link to the network server. *Any other person must get the express permission of a Director before taking any material in electronic form from the Company's premises* [my emphasis]'[177].

Some of the people who admitted doing such things[178] did not know that they were acting in breach of this policy – either because they did not know of the policy's existence[179] or were not sure what it stated[180]. So, for example, they did not realise that they were not in fact *authorised* to work remotely (via any means). Consequently, some people's actions were not actually 'workarounds,' because those

[176] See again section 6.4.6.
[177] See point 5 of Business B's *Use of Internet, Intranet, Email Access and Social Media Policy*, in Appendix A on page 159.
[178] For example, by sending work documents to themselves at home via their personal email accounts, or taking work away from the office on data sticks.
[179] P16, P17 and P25/B/DS.
[180] P12/B/DS.

people bypassed the formal path neither knowing of it nor the technological hurdles that lay down it. Rather, they chose their own path *solely* for the reason of 'just getting things done,' and often because busyness at work had prevented them from completing their work during office hours.

In Business C, the remote working policy prohibited the same types of behaviour, but did so implicitly[181]. Again, some people were occasionally doing these things to work around technical difficulties, while others were just doing them anyway. As the Office Manager explained: 'That's the sort of thing that people do' (P10/C/Int). The actions of those who do this without knowing that they are breaching a policy provide supporting evidence for the Finitist argument that practice is based on analogical experiences (Wittgenstein, 1967; Barnes, Bloor and Henry, 1996). Such people have not needed to know that there is a remote working policy, because they have never needed to refer to it before. They have just been doing what they do, to get things done. In short, Finitism buys into pragmatism.

It can be seen that – individually or in combination – busyness, the serving of immediate purposes and pragmatism often contribute to the shaping of people's rule-following behaviour, and the comments of two particular participants help to summarise and further evidence these facts. Speaking in general terms about cyber security at work, one said:

> 'If people have my mindset – and I'm sure that a lot of people do – when you're working, you just want to get on with your work, and get on with the job in hand; and often you're obviously not focussing on whether there might be a cyber security issue here or there' (P7/C/Int).

Speaking specifically about phishing emails, the other explained:

> 'It's just that, if someone phoned me and said: 'There's a funny email in your inbox. I've deleted it from my inbox ten minutes ago,' I would not really be concentrating on what they were saying. My day would have moved on. That probably sounds terrible' [P9/C/Int].

[181] Specifically, by listing the only two acceptable means of working remotely. The main way is via a remote desktop facility. The other way – to be used only where someone encountered problems with the main way – is via remote web access (by typing a specific URL into their web browser). These rules are found within Business C's *Notes on how to use Business C's IT system*; specifically, within the sections entitled 'Accessing the server remotely' and 'Remote web access.' See Appendix D, pages 175 and 176.

The important question is not whether that sounds terrible, but whether this behaviour is very unusual. The evidence suggests that it is not.

### 6.4.9 Interaction with others, and 'just what people here do'

The strongest of the influences on our rule-following behaviour is the people around us. As individuals, we often speak as if we are compelled by something outside of ourselves. But that something is not the rules, because, *in themselves*, rules possess no agency (Wittgenstein, 1967; Bloor, 1997). Our behaviour is shaped mainly by other people, by society itself. From these case studies came much evidence that within the workplace this social collectivity exerts strong influence upon whether and how people follow rules on cyber security. Rule-following is a *shared practice* in which we constantly modify our individual, habitual responses as we interact with others (Barnes, 2001).

Firstly, there was quite a lot of evidence that people interact with each other to seek and give informal advice on cyber security matters. This is interesting, not least because, while some of this is simply sharing formal advice that the advisee has either forgotten or not yet read[182], some is not. For example, a person in Business C said:

> 'Recently, I remember advising a colleague about how spam emails often pretend to be from Yahoo!, Barclays Bank or whatever, but you can check them by hovering over the [email] address' (P5/C/DS).

Although this advice was sound, it went beyond that given in the existing policy rules[183]. Another person in Business C reported giving work colleagues advice 'on how to use safe passwords' (10/B/DS), yet the policy rules gave no advice on how to construct safe passwords for devices and applications used for work purposes[184]. Both of these are examples of people giving cyber security advice from sources other than the businesses own policies[185]. On the matter of rule-following, both are examples of people telling their work colleagues what they themselves do, and recommending that their colleagues do the same. Also, each of them can be seen as cases of 'learned

[182] Examples include being told not to allow the web browser to save passwords (P6/C/DS), and being given advice on how to deals with suspicious emails and their attachments (P7 and P10/C/DS; P15, P16 and P18/B/DS).
[183] See the section entitled 'Dealing with spam emails' within Business C's *Notes on how to use Business C's IT System*, in Appendix D on page 177.
[184] See Business C's *Notes on how to use Business C's IT system*, in Appendix C on pages 175-177.
[185] And sometimes such sources might be dangerously inaccurate.

similarity relations' (Kuhn, 1977; Barnes, 1982), where someone is shown things, or ways of doing things, to which they then compare new things that they encounter and determine whether they are analogous. However, that person will be considered 'safe' only when their analogical reasoning is seen as consistent with that of other members of their community (Rees, 2011).

So, people seek and receive informal advice on *what to do*, but there was also evidence that they sometimes seek such advice on *whether to act*. For example, a person in Business B explained that: 'Sometimes, people will mention it if they have received an email that doesn't look right, and ask if anyone else has received the same or similar' (P14/B/DS). In such situations, people reported also being asked to give their opinion on whether it was a 'dangerous' or 'dodgy' email (P8/C/DS; P9/C/Int; P13/B/DS). On this matter, the policy rules of these three businesses provided little or no formal guidance[186]. So, in the absence of that, *necessarily* such informal advice was both sought and given. Consequently, in this type of situation some people are telling their work colleagues what they would do, and recommending that their colleagues do the same. Again here, there is evidence of learned similarity relations. In the absence of examples of which types of emails are 'safe,' the local community are sharing previously observed cases to develop a communitarian standard of 'safety,' which can then be used individually (Rees, 2011).

In the previous chapter, I presented evidence that in all three businesses there was considerable difference in the employees' awareness of *whether* policies existed on some key matters, and what was their *content*[187]. In turn, that difference in awareness and knowledge of policy will necessarily affect any informal advice given. Consequently, in perhaps a range of situations, some people will be doing one of two things: a) telling their work colleagues that they do not know what the formal policy is on a particular matter, but explaining what they themselves do, and suggesting they do the same; or b) informing them that there *is* a formal policy on that matter, and telling them what *they* understand that policy to be, and recommending that they follow it in that understood way.

[186] Only Business C had given formal policy guidance on how to spot suspicious (e.g. spam or phishing) emails. But that advice was very minimal. It simply stated: 'Even if an email is marked 'Internal,' it won't be – the spammers do this to try to fool people. And if an email in your Junk Box looks like it's from a member of staff, it won't be.' See the section entitled 'Dealing with spam emails' within Business C's *Notes on how to use Business C's IT system*, in Appendix D on page 177.
[187] See again section 5.5.2.

Here, it is important to note that consensus both shapes and drives rule-following behaviour (Bloor, 1997). So in these scenarios, when someone says 'this is what I do,' they likely mean 'this is what (I've been told) most people here do.' This becomes even more likely where in fact there is no formal policy on a key issue. Such was the case in Businesses B and C, neither of which had a policy/procedure on reporting risks and incidents that have either threatened or breached the business's cyber security. In interview, I first confirmed to each of the participants that no such policy/procedure existed formally within the business for which they worked. Then, I asked each of them what they would do if they became aware of such a threat to the business's cyber security. Their answers provide insight of the extent to which rules and rule-following are determined by consensus.

When I asked the Chief Executive of Business C this question, she replied:

> 'I would contact our IT Support company. And I'm pretty sure that's what all the staff would do….But it also flags up that we probably need to have a policy on it' (P4/C/Int).

In fact, her prediction turned out to be fairly accurate. Five of the seven other participants confirmed that they would contact the IT Support company[188]. However, it was interesting to note that three of them said they would *also* speak to the Office Manager (Participant 10), and that they would do this first *before* contacting the IT support company[189]. That could be because they know that the Office Manager is the person in most regular contact with the IT Support company. Indeed, the Chief Executive stated that 'they all know' that the Office Manager is the 'usual conduit' between Business C and that company (P4/C/Int). However, the comments of another participant suggest instead that these people would simply be applying a more general, everyday rule – itself created and maintained by consensus:

> 'I'd contact the Office Manager, because anything related to the office I would always report it to her. If I'm honest, I think it's because a lot of it is just common sense; because that's what everyone does, just report it to the Office Manager, whatever it is' (P7/C/Int).

[188] P5, P8, P9, P10 and P11/C/Int.
[189] P5, P9 and P11/C/Int.

This provides an example of rule-following being *what everyone does*, rather than any strict application of a written rule.

In Business B, the vast majority of the participants (16 out of 18 people) each said that the first thing they would do is contact the IT Manager[190]. Again, however, it was the reasons behind their 'choices' that were of interest, and these delivered more evidence of the presence and strong influence of a consensus on what is to be done. A few people said that they would contact him because he had asked everyone to report such things to him[191], and so, for them, this had become a firm (though informal) policy. As one of them put it: 'The general sort of day-to-day policy is that if there is any hint of a problem, then we refer it to the IT Manager' (P29/B/Int). But interestingly, another of them also said:

> 'If [the IT Manager] wasn't here, other than calling him repeatedly on his mobile phone, to be honest with you, I wouldn't know what to do. I'd probably make most people aware of it. But there's not anyone else that I would think: 'I need to tell this person, and they will deal with it.' I don't know what the fallback plan is at the moment, to be honest' (P16/B/Int).

Three other people said that they would contact the IT Manager 'just because…he's in complete control of all the systems' (P23/B/Int), which makes him 'the guy to go to' (P24/B/Int) and so 'everybody goes to him' (P13/B/Int). The rest of the participants mentioned that same reason, but cited other reasons as well. One of them spoke of physical proximity: 'I would go straight to [him] because he's in the office next door to mine' (P19/B/Int). Another person said: 'He always talks to us about cyber security, so he would just be the first person I would go to' (P27/B/Int); and someone else explained: 'I would report it straight away to [him]…because I know that over the last few months when it's been spoken about a lot, [he] has been the go-to guy' (P20/B/Int). This person added that he would probably also mention it to his Line Manager and to one of the Directors of the Business in order to, as he put it, 'cover my back' (P20/B/Int).

---

[190] P12, P13, P14, P15, P16, P17, P20, P21, P22, P23, P24, P25, P26, P27, P28, P29/B/Int. With regard to the remaining two Participants, one was the IT Manager himself (P18) and the other (P22) answered the question in the following way: 'I would probably bring it to the attention of my direct boss (i.e. Line Manager), the Head of the Department, who would then, I imagine, report it to the IT Manager. Just because she is higher than me in the hierarchy, I suppose' (P22/B/Int).

[191] P15, P16, P25 and P29/B/Int.

Notably, one person revealed that:

> 'The Directors aren't very tech-savvy themselves. If they were, I might report it to them first, instead. But there's a general acceptance that if someone receives something dodgy, they just forward it to the IT Manager and let him deal with it' P12/B/Int).

This was similar to the opinion of someone else, who said:

> 'I think that the obvious thing that people do when they get something suspicious is that they just tell the IT Manager, and he will advise them what to do. In essence, there is almost a way of dealing with it there' (P21/B/Int).

The final three people made reference to 'common sense,' amongst other things. One of them saw little need for formal rules on this matter, saying: 'Formal policy is different from using your common sense, and we've got a computer guy on site' (P17/B/Int). Another explained: 'You just follow a stream. It's not anything that I've been told to do, or I think is right. It's just what I believe is common sense' (P26/B/Int). Lastly, the comments of one participant encapsulated much of what had been said collectively by the others:

> 'I base my knowledge of this on a general understanding of what is going on…I think that the policy, which I am going to say is implicit or that I understand to be what would happen, is: Don't try and do anything yourself, go and speak to the expert. Maybe it's just common sense…But there is a culture, for want of a better word, in how to deal with this. It's not as if we wouldn't know what to do' (P28/B/Int).

In essence, she was saying: this is just what people here would do. So, practice can be done rightly or wrongly, but these normative standards are set and maintained by *consensus* within the whole group of interacting rule-followers (Bloor, 1997). In short, the *community* decides what is, and what is not, successful rule-following behaviour.

### 6.5 Conclusion

In this chapter, further findings from my case studies have been discussed. These findings have included the discovery of certain views among the senior management of these three businesses on rules and rule-following behaviour around cyber security.

It has been argued that these views sometimes feature very questionable assumptions. In place of them, I have called for a more enlightened view of these matters, based on a Rule Scepticist reading of Wittgenstein's thoughts on rule-following, and my findings have provided much evidence to support that view by showing the realities of rule-following behaviour in everyday working life. More specifically, these findings do two things: Firstly, they challenge strongly the notion that people's rule-following behaviour around cyber security is determined mainly by the language in rules, which always shows them the way. And secondly, they provide much evidence of what are often the *true* influences on people's rule-following behaviour. These have been found to include personal traits and tendencies, personal interest and lack of interest, personal perspectives on technology and cyber security, professional experience and job status/level, workload and work time pressure, technological obstacles and possible 'workarounds', the anticipation of formal sanctions, busyness, the serving of immediate purposes, and interaction with others. In particular, the last three of these were found to be very potent influences on whether and how people follow policy rules on cyber security. The evidence suggests that people's rule-following behaviour is shaped mainly by two things, combined: consensus and pragmatism. Consequently, behaviour is often being driven by collective agreement between work colleagues about what should be done, and how, and with what considerations in mind; and in reality, that often boils down to 'just what people do here' in pursuit of 'getting things done.'

# Chapter 7: Discussion

## 7.1 Introduction

In this chapter, I will discuss the full evidential picture that has emerged from my research. That picture provides a more enlightened view of the evermore important task of governing people's behaviour around cyber security. My discussion of it will include calls for change in the government's thinking, and its advice to the business sector. It will also set out ways to solve the problems of responsibilising employees for cyber security within small businesses. In short, it will demand top-down changes and provide bottom-up solutions.

## 7.2 The complexities of responsibilisation

Risk management is seldom easy. Since 2011, the UK government has been seeking specifically to manage the risk(s) of cyber insecurity. As a major part of this, it has been trying to get businesses to improve their employees' behaviour towards cyber security. Continuing a post-modern trend of governance, the State has sought mainly to do this from a distance, by steering rather than rowing. Essentially, that has involved the responsibilisation of businesses in the fight against cybercrime. Conscripted into this difficult ongoing battle, those businesses face what I have termed the 'responsibilisation conundrum': getting all of their employees to behave securely, all of the time.

Within this strategic approach, the government has continued to sharpen its focus on SMEs, urging them to harden themselves as targets. That has included telling SMEs to responsibilise their own employees in matters of cyber security, and advising SMEs on how to do this. However, the government continues to be frustrated with what it sees as a poor response to those demands and to that advice.

Certainly, any form of risk management carries with it a blaming system (Sparks, 2001; Garland, 2001). However, the government's continuing strategy on cyber security – built around the responsibilisation of businesses and individuals – has also delivered the danger of victim blaming. Shifting the focus unduly from the criminals to the victims, such blaming can also lead to businesses/people being denied the status of *legitimate* victim, with potentially heavy costs (financial, legal, reputational). Arguably, that danger is greater in this particular field because, among the causes of

any cyber security incident, some (in)action by the victim can usually be found. This then enables the government and others – employers, business partners, lawyers, insurance companies – to say: we warned you about this risk, and told you how to avoid it, but you did not practise what we preached so you must shoulder or share the blame. But these preferred governmental strategies are, at best, limited. For instance, there is the possibility that the cyber insurance market will be slanted against small businesses, because they will tend to struggle to achieve victim status, and so their insurance premiums will remain too high. This forms part of a wider, developing picture in which there are now fewer victims of cybercrime because 'ideal victimhood' is being used as the yardstick for legitimate victim status.

Within its rhetoric of responsibilisation, marked increasingly by vehemence and frustration, the government has also been shaping victim status, and thereby making it even more difficult for businesses/people to attain that status of legitimate victim. In turn, this also increases the potential for victim blaming. The pressure from government continues to increase, not least from its stated intention to implement the EU's General Data Protection Regulation (GDPR) in May 2018 (HM Government, 2016c; DCMS, 2017c). This will impose upon businesses more onerous duties concerning data protection[192], and bring with it the spectre of much heavier financial penalties for non-compliance[193].

All of these pressures on businesses – a greater range and potency of cyber security threats, gaining and retaining insurance against them, more onerous legal duties, and thus greater potential for litigation – will mean that, in turn, those businesses will place considerably more pressure on their own employees to comply with cyber security policies, all of the time[194]. But my research has shown that government thinking on this matter is mistaken. Lack of insight continues to affect the quality of

[192] Including the legal requirement to notify individuals (and government) of cyber security attacks that compromise personal data and are likely to result in a risk to people's rights and freedoms.
[193] Thus far, the largest fine for breaches of data protection in the UK has been £400,000. This was imposed by the Information Commissioner's Office (ICO) on *Talk Talk* plc in November 2016 (BBC, 2016b). Certain breaches of the forthcoming GDPR legislation could result in a business being fined up to €20 million (£18 million), or 4% of its annual worldwide turnover, whichever is the greater – Art.83, GDPR.
[194] It is worth noting here that, in line with the previous year's findings, the government's Cyber Security Breaches Survey 2017 found that only 33% of businesses had a formal policy on cyber security, and that only 32% of businesses had cyber security risks documented in business continuity plans, internal audits and risk registers (DCMS, 2017a, p.30). However, it is submitted that businesses' policy formation on cyber security will only grow within the climate of ambient pressures just mentioned. Indeed, the survey also reported that smaller businesses are now more likely to have formal cyber policies in place, given 'the increasing importance [which they] now attach to cyber security' (Ibid, p.30).

the advice that it gives to businesses, leading to business strategies that are misguided and have little chance of success.

### 7.2.1 Why government advice and business strategy must change

The task of responsibilising individual employees for cyber security is one which the government seems to think is demanding, yet relatively straightforward. It continues to advise businesses to achieve it by informing and training employees about cyber security, and monitoring, restricting and disciplining their behaviour around it. However, my research has shown, not only that the government is underestimating this task, but that *the task itself* is even more difficult than previous research suggests.

The second and third stages of my research revealed two crucial things: Firstly, that government advice to businesses on how they should responsibilise their employees for cyber security, and businesses own approaches to it, lack understanding of the complexity of that task. And secondly, how important Meaning Finitism and Rule Scepticism are to the understanding and performance of that task, and to the subject of cyber security in general.

### 7.2.2 The complexities of shaping and controlling employees' behaviour around cyber security

Together, training and the use of policy rules are the two main ways of influencing the human aspects of cyber security. My research has shown that truly effective use of these means is more much complicated and challenging than the government perceives it to be.

Assumptions about employees' lack of interest in training are easily made, but my research found that most people welcome formal guidance on cyber security from their employers. However, it also found that, in practice, the provision of such guidance can be beset with problems. Firstly, humans differ, and so do their training needs. At times, there was evidence that a one-size-fits-all training model can lead to dissatisfaction, corroding engagement with it. Indeed, sometimes people can begrudge what they see as mismatched training cutting into their worktime. Also, evidence was found of 'training fatigue.' People can become weary of, or frustrated with, attempts to train them in cyber security, and this tends to make them much less

responsive to such training. It can stem from information overload, too frequent training, or 'friction' with personal workloads – or any combination of the three.

Here again, personal preferences were found to be important. Of the three businesses, Business B delivered the most cyber security training to its employees, and it was the only one to employ an IT Manager in-house. He took care in his design of that training, convinced as he was that the employees 'would like to gain more knowledge on [cyber security], without having to put a lot of effort into doing so' (P18/B/Int). That resulted in the training being delivered only by him, and mainly by email. But this was far from a success. Alongside problems of 'training fatigue' and 'friction' – where many people would ignore, or just delete, such training emails – there was much evidence that this approach was doomed to fail from the start, because most people simply disliked it as a means and mode of training. Indeed, across all three businesses, diversity was found in people's views on how they would like to be trained in cyber security. Different people want different things, depending upon their own personal frictions, tendencies, attitudes and experiences.

So, on this matter of training, government thinking and advice is disconnected from everyday practice in two important ways. Firstly, the government seems to view the task of training employees in cyber security as being onerous, but not very complicated. My research has shown instead that, for a range of reasons and in a number of ways, it can be truly problematic. And secondly, given the diversity that I found in people's training preferences, and other research which has shown that training is more effective when it is personalised (Mangold, 2012), the government may have underestimated the heavy influence that financial pressure can exert on cyber security training within small businesses. Even where financial problems have not precluded or displaced plans for such training (e.g. as they had done in Business A), that proven diversity in training preferences makes training even more problematic, specifically because for several reasons (e.g. cost and continuity/coverage of work) many small businesses could never afford to introduce bespoke training methods to suit their employees' individual training preferences and needs.

The issue of governing behaviour through rules has been the particular focus of my research. It is a matter on which the government continues to urge businesses to do better, and do more (e.g. DCMS, 2017b, p.2). Again, I found evidence that financial

pressure can affect such plans. For example, in Business A the daily tasks concerning business survival had taken priority over the creation of formal policy rules on cyber security. The owner of the business thought it important, but explained that 'it's one of these things that is a job that's constantly getting postponed' (P1/A/Int).

Within the other two businesses – both of which had formal policy rule sets – a number of people lacked awareness of policies, or their specific content. More importantly, where policy was known to exist, there was much evidence of the more challenging problem of *disengagement* from it. There were found to be several causes of this. People can disengage through 'rule fatigue,' feeling pressured by the burgeoning number of rules and their growing content, and/or by the 'friction' they cause with the performance of primary work tasks. Also, too much reiteration of policy can lead some to disengage from it through 'reminder fatigue.' There was evidence that when people feel bombarded by communications on cyber security policy this can alienate them from the subject, or make them ignore it (for a while, at least), thereby increasing the risk of mistakes and other insecure behaviours. And lastly, as in training, dissemination of the information can be problematic as well. I found that people's individual preferences for how policy should be delivered to them varied significantly, bringing the danger that some people may disengage, either occasionally or continually, from some or all aspects of certain policies.

These problems alone make this task much trickier than the government seems to think it is. However, my research has also revealed *much deeper* problems, which challenge previous thinking on the use of rules in governing people's behaviour around cyber security. These were discovered because the collected data delivered a lot of evidence of the *true* influences upon people's rule-following behaviour, and the importance of Meaning Finitism and Rule Scepticism in the understanding of those deeper problems and that behaviour.

These research findings expose as flawed some assumptions that were being made by the senior management in these three businesses about rules and rule-following behaviour. More specifically, the findings challenge strongly the notion that people's rule-following behaviour around cyber security is determined mainly by the rules themselves, and provide instead much evidence of what is *actually* influencing their behaviour. Those influences were found to include personal traits and tendencies, personal interest and lack of interest, personal perspectives on technology and cyber

security, professional experience and job status/level, workload and work time pressure, technological obstacles and possible 'workarounds', the anticipation of formal sanctions, busyness, the serving of immediate purposes, and interaction with others.

The key findings were that people's behaviour around cyber security is shaped mainly by two things: firstly, by pragmatism – a keen pursuit of just 'getting things done'; and secondly, by normative standards that are set and maintained through consensus by the people around them, and which determine what is, and what is not, 'correct' rule-following behaviour.

Here again, government thinking and advice is disconnected from everyday practice. This time, through the same lack of understanding of rules and rule-following behaviour displayed by the senior management of these small businesses, and by a similar lack of awareness of what is truly influencing employees' behaviour around cyber security in their everyday work.

### 7.2.3 Can any of these findings be generalised?

It is important to note that, necessarily, most of these findings cannot be generalised to the small business sector as a whole within the UK. There are several reasons for this. Firstly, since the findings were made within just three small businesses, the same type of research would need to be conducted in a number of other such businesses, and similar findings made, before any credible generalisation could follow. Secondly, each of those three small businesses is situated in the same area of the UK (the English county of Hampshire). This geographical clustering also hinders any attempts at generalisation. And lastly, those three businesses were operating in different business sectors. Such sectoral diversity prevents any generalisation as well.

However, it is submitted that some generalisation can be made from some of these research findings. Specifically, those that will now be discussed within the first paragraph of the next section (i.e. findings concerning the tension between government policy and everyday working practice, and flaws implicit within the existing rule-heavy, top-down strategic approach towards cyber security within small businesses).

### 7.3 Given these new findings, what should be done?

My research has revealed an inherent tension between, on the one hand, government policy on responsibilising businesses and their employees for cyber security, and on the other, the realities of everyday working life. The model selected and being determinedly pursued by government is one in which rules feature heavily. Examples include the *10 Steps to Cyber Security,* the *Cyber Aware* campaign (formerly *Cyber Streetwise*), the *Cyber Essentials* accreditation scheme (now also linked with cyber insurance), and continuing calls for the creation of more cyber security policies within businesses (e.g. DCMS, 2017b, p.2). But my research has also shown that it is almost impossible to impose this form of governance from above, either from government level or senior management level.

Within that rule-heavy model, *in practice* cyber security is being undermined, not because people are being lazy or selfish etc., but because of a rich set of influences on rule-following behaviour, the most potent of which are community-based norms and conventions concerning ways of following rules in time-pressured situations. The reality is that routine, everyday, sociological factors are driving rule-following behaviour, not the rules themselves. Given all of this, government policy and business strategy on these matters should change to reflect these truths, and the existing rule-heavy model should be replaced by one newly-designed.

#### 7.3.1 A new way of responsibilising employees for cyber security within small businesses

One of the things that a Finitist understanding of rule-following behaviour shows us is that the creation of more rules is not the answer to the 'responsibilisation conundrum.' Indeed, further findings from my research provide yet more evidence of this: I discovered that when certain policies were absent[195], employees were pursuing collective practice *anyway*, governed by their *own* agreed set of rules. This demonstrates that when there is a pre-existing culture of 'safe' practice[196], formal rules may not be needed anyway. It also indicates that, rather than having

[195] Particularly, for example, where none of the three businesses had a formal policy for reporting risks and incidents which are thought to have either threatened or breached their cyber security.
[196] In this context, the term 'safety' is used to refer to 'the ability of [someone] to make similar claims to their peers, and is related to the correlation of [that person's] classifications to those of other members of the community' (Rees, 2011, p.869).

reductionist rule sets – which themselves will never capture adequately the multiplicity of cyber security threats – much more emphasis and effort should be put into embedding a 'cyber security culture' within small businesses. One in which, *inter alia*, all employees are trained regularly through a Finitist approach, using exemplars and case studies within group discussions.

Finitism shows us that rules themselves can neither guarantee their own future application nor the way in which that is done. This is because the terms used in rules lack inherent meaning, and have been used only so many times. Consequently, there is always a 'next step' to be taken (Wittgenstein, 1978), which means that rule-following proceeds on a case-by-case basis, and the terms within the rules are *given* meaning each time they are *used* (Wittgenstein, 1967). Within the context of cyber security, my research has revealed the most potent influences upon such use of rules, delivering evidence that rule-following is very much a *shared practice* in which we constantly modify our own responses as we interact with others (Barnes, 2001), and that collective consensus both shapes and drives our individual rule-following behaviour (Bloor, 1997). In short, that it is a sense of community which actually enables rule-following to happen.

Given these findings, I am recommending a new approach to the tricky task of shaping and controlling employees' behaviour around cyber security within small businesses:

### 7.3.2 A two-stage solution to the 'responsibilisation conundrum'

In essence, the solution to this problem is the weaving of cyber-secure practices into the fabric of everyday work processes. Necessarily, this is a bottom-up solution, and should be done in two key stages:

To begin with, and set against the backdrop of its current rule set and training regime, there should be an investigation into the practices around cyber security that are *actually* taking place in the business (i.e. 'what we do here' and 'why we do it in these ways'). This behaviour will have been influenced by a number of things, but mainly by standards set and maintained by the community of people working for the business. To obtain data that is accurate, it is crucial to collect it through processes seen to be non-judgemental and blame-free. Data collection methods should include one-to-one interviewing, accompanied by a guarantee that the interviewees' responses will be protected by anonymity. Ideally, this investigation should be conducted by one

person, who is neither the IT Manager (if the business employs one) nor a representative of the IT Support company (if the business uses one), nor a Senior Manager. However, once collected, the data should be given to them, and to the senior management of the business. It will tell them what people are doing, what they are not doing, and why. With this information, they can then plan the next stage.

The second stage of the solution is to train the employees in a Finitist way. Such training should be based on the 'knowing cases' model that has been used in other areas of education, such as Biomedicine (see, for instance, Sturdy, 2007) and Forensic Medical Examination (see Rees, 2011). Within its Finitist account of training, Rule Scepticism has relied heavily on the work on Thomas Kuhn. In essence, Kuhn argued that scientific knowledge comes from exemplar-based puzzle-solving (Kuhn, 1970). In other words, it is knowledge of cases; specifically, exemplary cases of puzzle-solving (Sturdy, 2007). The use of exemplars[197] and case studies within cyber security training is the key to influencing the behavioural standards set collectively by the employees themselves, and how that community polices itself.

This 'knowing cases' model of training is best conducted within small groups. Other findings from my research have shown that most people would prefer to receive face-to-face training in cyber security, and preferably in small group sessions[198]. Again, this points to that sense of community. Indeed, it seems that many of them would also welcome the use exemplars and case studies within that format, including the use of real-life examples. For instance, one participant said:

> '[W]hen it's a story about someone else – like one recently of a Solicitor who was tricked into transferring over clients' money – it makes you realise how real it is, and how current it is….[and] that it could happen to you, and here's an example of it' (P14/BB/Int).

Another thought it best to 'have an opportunity…to discuss best practice, discuss individual case studies, actually as an interactive session' (P28/BB/Int), and someone else considered that 'small group meetings would work, with updates and visual examples…..And I think that real-life examples always help as well' (P12/BB/Int).

---

[197] Kuhn used the term 'exemplar' to describe any firm solution to a problem which is 'accepted by the group as being, in a quite usual sense, paradigmatic' (Kuhn, 1977, p.298).
[198] P1/A/Int; P6, P8, P9, P11 and P12/C/Int; P12, P19, P21, P22, P23, P26, P27, P28 and P29/B/Int.

Membership of these small training groups should not be determined by random selection. Instead, thought should be given to bringing together people from different levels and types of employment within the business. Also, group membership should be changed, but not too often.

The training should be delivered by the IT Manager (or equivalent), or by a Senior Manager. In this way, the desired normativity (i.e. the correct, cyber-secure ways in which to behave) can be pushed regularly by the power of authority. Ideally, the same person should run all of the training sessions. However, the use of guest speakers and other contributors can also help to train people well. Training sessions should be regular, but not long. Also, each of them should be a friendly, open environment in which people feel free to talk and to learn. So, for example, in a typical training session, together people might work through and discuss an exemplar or case study, be updated with examples of current cyber security threats, share recent experiences and practices, and (crucially) ask questions.

The key advantage of this model is that it taps into, and then influences, that sense of community which is the real driver of rule-following behaviour. Further advantages are that it can be done relatively cheaply, and quickly.

In summary, this recommended new approach to training and guiding employees about cyber security comprises:

**Stage 1** **Investigate current cyber security practices within the business**

- This investigation to be conducted by one person (but not the IT Manager nor a Senior Manager), using one-to-one interviewing among the methods of data collection.

**Stage 2** **Take a Finitist approach to training**

- The design and delivery of this training to be based on the 'knowing cases' model, using exemplars and case studies (including real-life examples).
- All of this training to be delivered/coordinated by one person, who is either the IT Manager (or equivalent) or a Senior Manager.
- Training to be delivered in small groups sessions. Six people per group is suggested as an appropriate number.

- The suggested length and regularity is one half-hour training session per month.
- Group membership should reflect different levels and types of employment within the business, and not be subject to frequent change. The suggested regularity of change is once a year.

### 7.4 Conclusion

Cyber security is part of everyone's daily lives now, part of what everyone *does*. However, there needs to be a recognition that it cannot be managed from the top down. Rather, any management strategy should be grounded in the lived experiences of cyber security within everyday working life. Together, Meaning Finitism and Rule Scepticism show us that if you do not control the way that information is diffused in small communities, while certain practices may be deemed 'correct' within those communities, they may not also be safe. Instead, I am recommending a new approach to this task, as part of a solution to the 'responsibilisation conundrum' within cyber security, featuring a normative dimension which ensures – through the use of exemplars and case studies within small group discussions – that the 'correct' way to do things is also the secure way to do things. Through it, this desired normativity can be pushed regularly by the power of authority (e.g. IT Manager or Senior Manager), shaping and re-shaping employee behaviour towards cyber security during their daily work within small businesses.

# Chapter 8: Conclusion

## 8.1 Key findings and Conclusions

Essentially, this thesis is the result of an investigation into the use of words. More specifically, words used to prompt and shape conduct around cyber security. In the first stage of my research, I looked at the words of recent governments, often used to tell citizens and businesses what actions they should be taking. In the second and third stages of my research, I looked at the words used by businesses when trying to control the behaviour of their employees.

First, I was keen to explore the political context in which the matter of cyber security sits. Specifically, I wanted to determine whether cyber security is a policy area where the State continues to push responsibility away from itself and onto non-State actors, as a means of extending and enhancing the governance of situations and environments which have a tendency to produce criminal behaviour (Garland, 1997). My detailed analysis of much government discourse on cybercrime and cyber security confirmed very much that it is. The government continues to speak with increasing vehemence about the responsibility of businesses and individuals to protect themselves (and others) from cybercrime. In fact, its chosen words have become more judgemental and less tolerant, through frustration with what it sees as poor risk management by those responsibilised actors.

My documentary analysis unearthed other things as well. I found that, through its discourse, the government is shaping victim status, often seeming to restrict this to the 'ideal victim.' In turn, this increases the risk of victim blaming, a danger known to lurk within the responsibilisation and target hardening elements of the Neoliberal approach to the management of risk. Indeed, I found examples of victim blaming by near-government organisations, such as banks and the police. My findings suggest that as the clamour for responsibilisation within cyber security grows – driven mainly by the government – so too does the risk of victim blaming. In this way, the government's continuing strategy of responsibilisation, and its choice of words in pursuit of that strategy, are complicating the claiming of *legitimate* victim status, and the consequences which can flow from gaining, or failing to gain, that status.

I discovered also some additional pressures that are shaping perceptions and policy around cyber security in the UK. These include the fact that much cybercrime feeds further criminality, so that many instances of cybercrime victimisation can be ongoing and onward. Consequently, people and businesses are now viewed not only as potential victims to cybercrime, but as potential (unwitting) accomplices to it as well. In turn, this hardens the responsibilisation rhetoric from government down to (and between) businesses, and on to employees. Also, the issue of cyber insurance is looming larger, driven on and supported by the government. In due course, that will further complicate and contort the matters of victim labelling and victim blaming. And lastly, the government will soon impose upon businesses more legal duties concerning cyber security and data protection, mirroring those within new EU legislation as the UK nears its departure from the European Union[199].

In this way, the first stage of my research confirmed that the UK government continues to employ a responsibilisation strategy in the governance of cybercrime and cyber security, yet appears increasingly annoyed by that strategy's failings – for which it seems to blame those whom it has responsibilised. In the second and third stages of my research, I was keen to evaluate that strategy, through investigation of its implementation 'on the ground.' In particular, I wanted to learn how small businesses are coping with what seems a tricky task, passed on to them by the government: that of getting *each* of their employees to behave in cyber-secure ways, *all* of the time. This 'responsibilisation conundrum,' and the challenges which lie in seeking to solve it, have been the main focus of my research.

One of the initial findings from my small business case studies was that most employees would welcome further guidance on cyber security, if done well. But I also found that the provision of such guidance can be beset with problems. Sometimes, financial pressure can preclude or displace plans for it. When it *is* provided, the training needs of employees will likely differ, but financial cost may limit the training to a 'one size fits all' model, causing some to begrudge its low pitch and slow progress, and so deem it a waste of their (busy) working time. This can also undermine the creation and sustainment of a culture of cyber security within a business. Other

[199] The UK is scheduled to leave the European Union in March 2019. Meanwhile, in May 2018 the UK government will bring in legislation to implement the provisions of both the Network and Information Security (NIS) Directive 2016 and the General Data Protection Regulation (GDPR) 2016.

problems that I found include 'training fatigue,' induced by information overload, or too frequent delivery of training, causing people to become anxious that it is cutting too deeply into their worktime. I discovered also that employees' individual preferences for *how* they should be trained, and what should *feature* in that training, can differ significantly. But again, particularly in small businesses, financial cost can present a real barrier to catering for choice.

Guidance through policy can also be very problematic. Sometimes, if a business is struggling financially, the creation of cyber security policies can sit low on its list of priorities. However, paradoxically, the cyber *in*security which this brings can further threaten the business's survival. I found also that, even where policy exists and people are aware of its content, there may be several reasons why they may still disengage from it. Strong amongst these is people's individual preferences for how policy should be delivered to them. Another is 'reminder fatigue,' brought on by being bombarded with communications about cyber security, and feeling alienated from that subject, increasing the risk of insecure behaviours. Employees can also disengage through 'rule fatigue,' as the number of rules and their content increases. Often, this can result from 'friction' between those rules and their primary work tasks.

Collectively, these findings from the case studies indicated strongly that the government has underestimated the difficulty of that crucial responsibilising task which it has delegated to all private sector businesses, 99.3% of which are small businesses (Federation of Small Businesses, 2016). Specifically, by showing that the governance of employees' behaviour around cyber security, in and beyond the workplace, can be far from straightforward, mainly due to its financial cost and the 'friction' it can cause with those people's work.

However, my research has gone on to demonstrate that this task of responsibilising individuals for cyber security is *even more difficult* than has been recognised before, by the government or anyone else. Specifically, because the matter of rules and rule-following behaviour brings greater complexity to it. Two aspects of my research have combined to shed new light on the 'responsibilisation conundrum': Firstly, further findings from the case studies have provided much evidence of the *real* influences on people's rule-following behaviour around cyber security, the most potent of which were found to be pragmatism ('just getting things done') and consensus ('that's how we all do it here'). And secondly, the first application of Meaning Finitism and Rule

Scepticism within the subject of cyber security has challenged strong assumptions being made by government and businesses about the efficacy of rules and their use in the governance of cyber security. It has also delivered a deeper understanding of rule-following behaviour within this discipline.

Together, all of the evidence from my research supports the two main conclusions of this thesis. The first of these is that the government's current strategy is flawed, because the government itself does not understand the true complexity of the 'responsibilisation conundrum' which it is demanding that businesses solve. Consequently, its advice to businesses on this, and their resulting approaches to it, are flawed as well. In particular, because they place too much faith in the efficacy of rules as a means of governing people's behaviour around cyber security. That lack of insight, and this mistaken thinking that comes from it, is producing business management strategies that are misguided and have little chance of success. In light of this, the second main conclusion is that those strategies should be subjected to *informed* change. Insights from Meaning Finitism and Rule Scepticism, combined with and applied to this new data concerning the *real* influences on people's rule-following behaviour around cyber security, make clear which changes are needed:

### 8.2 Policy recommendations

The first recommended change is that in future any strategies for governing the human aspects of cyber security should be *grounded* in people's lived experiences of cyber security within their everyday working lives.

This second is that, as part of a solution to the 'responsibilisation conundrum,' a Finitist approach should now be taken to training and otherwise guiding people towards cyber-secure behaviours. Combining a true understanding of the relation between rules and conduct, and a recognition of the multiplicity of cyber security threats, this is an approach that will help shape the behaviour of employees in ways sought but seldom achieved by rule-setting.

It is important also to view these two policy recommendations in the light of some very recent signs of change in government thinking that will be discussed in the next section (8.3). Henceforth, the government should be advising all stakeholders to adopt this more enlightened approach to cyber security. More specifically, it should tell all businesses in the UK – the vast majority of which are small businesses – that a

successful, secure business organisation is one which, *inter alia*, better understands its employees and the role that each of them play in its cyber security; in particular, the role that they are *able* to play, and *how*.

### 8.3 Encouraging signs of change in the government's perspective

This very month (September 2017), evidence has emerged of some positive change in government thinking about cyber security, specifically in relation to the human aspects of it. Finally, the government seems to be recognising – and is taking on board – the important findings from years of Human Factors research. In his speech to the CBI in September 2017, Ciaran Martin (the CEO of the National Cyber Security Centre) said:

> 'So, let's get serious about understanding the human being in all of this. Let's stop talking nonsense about humans being the weakest link in cyber security; it's a bit like saying that the weakest link in a sports teams is all the players' (National Cyber Security Centre, 2017a).

He then went on to quote, from one piece of that academic research, the key Human Factors principle of 'fitting the task to the human,' in pursuit of Usable Security (Pfleeger *et al*., 2014). These are encouraging signs. Hopefully, this will make it more likely that, alongside its recognition of findings within the Human Factors stream of research, the government will be more interested in, and open to, other research findings within the human aspects of cyber security, such as those presented in this thesis.

### 8.4 Future work

The three small businesses in which I conducted the case studies differ in two main ways. Firstly, each comes from a different business sector: Business A is a marketing firm, Business B a law firm and Business C a charity. And secondly, they each employ a very different number of people: 3 in Business A, 47 in Business B and 21 in Business C. This diversity was a positive feature for my research, in that it allowed me to compare and contrast the cyber security challenges, strategies and practices within different-sized organisations, operating in different business contexts.

However, in future research it would be valuable to conduct similar studies within a much greater number of small businesses. One of the benefits of this would be to

enable investigative comparison of businesses that are *similar* in size and nature; and this could be in addition to continued, deeper comparison of businesses that differ in these ways. For example, case studies could be conducted within three main research groups. Each group would comprise similar businesses, but each group category would be different[200].

It would also be useful to widen the research geographically. The three small businesses in which I conducted these case studies were all located in the same part of the country (Hampshire). Those future studies could be conducted, for example, in three different regions of the UK. Amongst other things, this might provide insight of the degree and quality of support that is made available to small businesses on the matter of cyber security by, for example, regional offices of the Federation for Small Businesses and the British Chamber of Commerce, and the police's Regional Cyber Crime Units (RCCUs) [201].

All of the data that I collected during the case studies was qualitative. In that future work – involving many more research participants – it would be beneficial to collect some quantitative data as well. For example, data on gender, age, education, nature of job, level of employment, and degree/type of training in cyber security received. This extra data could be gathered within one, or across all, of the same research methods (Observation visits, online Diary Study, and follow-up Interviewing).

Lastly, and just as importantly, in other future work the same kind of case study research should be conducted within a range of *medium-sized* businesses. In addition to determining whether the findings and recommendations made in relation to small businesses also hold true in those bigger businesses, it would enable the discovery and

[200] E.g. Group A = 10 businesses operating in business sector sector X, each employing approximately 5 people; Group B = 10 businesses operating in business sector sector Y, each employing approximately 20 people; Group C = 10 businesses operating in business sector sector Z, each employing approximately 40 people.

[201] These Regional Cyber Crime Units (RCCUs) sit within, and are supported by, the Regional Organised Crime Units (ROCUs), of which there are nine (South East, South West, Southern Wales, Eastern Region, West Midlands, East Midlands, North West, Yorkshire and Humberside, and North East). The role of RCCUs is described by the National Crime Agency in the following way: 'RCCUs increase cyber awareness across their local police forces, community safety programmes and criminal justice partners. They create local partnerships with academia and industry, in order to develop synergies in cyber capability around prevention of, and response to, cyber incidents. They help regional industry protect itself from cyber crime, through the creation and facilitation of regional information-sharing partnerships' (National Crime Agency, 2015, p.3).

analysis of any *different* cyber security challenges, strategies and practices within them.

# List of Appendices

The following thirteen documents have been appended to this thesis:

**Appendix A:** **Redacted copies of the relevant sections of Business B's Office Manual** – page 155.

**Appendix B:** **Business C's Social Media Policy (extracted from its Staff Handbook)** – page 166.

**Appendix C:** **Business C's ICT Induction Document** – page 171.

**Appendix D:** **'Notes on how to use Business C's IT system' Document** – page 175.

**Appendix E:** **Listing of the thematic framework used in the Documentary Analysis** – page 178.

**Appendix F:** **List of the twenty-five documents analysed during the Documentary Analysis** – page 179.

**Appendix G:** **The data from the Documentary Analysis set with the thematic framework** – page 183.

**Appendix H:** **Listing of the thematic framework used in the analysis of the data collected during the Case Studies** – page 208.

**Appendix I:** **The data from both stages of the Case Studies (Diary Study and Interviewing) set within the thematic framework** – page 209.

**Appendix J:** **Recruitment Advert** – page 241.

**Appendix K:** **Participant Information Sheet** – page 242.

**Appendix L:** **Consent Form** – page 244.

**Appendix M:** **Diary Study Questions** – page 245.

# Appendix A **Redacted copies of the relevant sections of Business B's Office Manual.**

## 1.10 Data Protection

We must comply with the Data Protection Act 1998 ('the Act') in our handling and storage of all data, whether on computer or otherwise. This includes data on employees, clients and others, in accordance with our registration with the Data Controller.

### 1.10.1 Registration

It is the responsibility of the Finance & Operations Manager to ensure that:

- the Company is registered for all necessary activities under the Act
- there is a process of quarterly review to determine whether any changes in the Company's registration are required as a result of changes, or planned changes, in the nature of the business
- the details of the Company as registered are kept up to date

### 1.10.2 Data Protection Principles

We must ensure that all data covered by the Act (which includes not only computer data but also personal data held within a filing system) is:

- fairly and lawfully processed
- processed for limited purposes
- adequate, relevant and not excessive
- accurate
- not kept for longer than necessary
- processed in accordance with the data subject's rights
- secure
- not transferred to other countries without adequate protection

### 1.10.3 Codes of Practice

The Company will observe the codes of practice provided under the Act. These may be altered or added to by the Information Commissioner, who is responsible for the administration of the Act. Applicable codes apply to:

- use the by Company of CCTV cameras
- various aspects of employment practice, including:
- recruitment and selection
- records management
- monitoring at work
- medical information

The applications of these Codes of Practice which relate to employment are dealt with in Section 3.

### 1.10.4 Subject Access Requests

Any individual whose data is held by the Company may make what is called a 'subject access request' – i.e. a request to see what data we actually hold about them. All such requests should be addressed in writing to the Finance & Operations Manager, who will ensure that the necessary arrangements will be made. For full details see paragraph 3.24.

### 1.10.5 Security of Data

This may mean electronic or physical security, or, as with a laptop computer, both. Employees must comply with the Company's IT policies. In particular, employees must observe secrecy in respect of their username and password. Access to any part of the Company's network must not be granted to any unauthorised person. If teleworking or working on a computer at home, or using mobile phones, Blackberries and iPhones, employees should take extra care PCs must be turned off at close of business every day with all applications closed.

## 3.3 Electronic Communications

The company operates a strict policy in respect of electronic communications. All employees must familiarise themselves with this. Please refer to Appendix 19.

## 4.1 Word Processing

The Company's word processing function is by way of fully integrated Microsoft Office 2007/2010 standard, or Windows 7 all with Outlook, Word and Excel. The PCs are networked to be a file server and each PC shares access to files held on the file server, unless protected by a password. The IT Manager is available to advise on procedures.

A fully integrated case management, Financial, IT processing system specifically designed for solicitors is in operation – Videss.

1. Members of staff should never install any software without the permission of the IT Manager – this includes screen savers. Doing so could affect both software and hardware and data is already installed on the system, or could introduce a virus.

2. Members of staff should never change a precedent on the system without specific consent of the head of their team

3. Members of staff should notify the IT Manager if there are any problems relating to the software or the hardware on their terminal. "Superusers" for the following application have been appointed:

   Videss - xxxxxx (Case Management). xxxxx (Case Management) xxxxxx (Financial set up) and xxxxxx (Financial, Time Rates, set up, apporvals/authorisation for users);

   Word - xxxxxxx

   Excel - xxx, xxx and xxx

   PowerPoint - xxxxx

   Users should refer to the above Superusers for simple 'how to' queries in the applications listed. This ensures that the IT Manager's time is used to full effect in maintaining the overall systems.

4. Whenever a paper is closed, all that material should be deleted from the system, except for precedents and account matters. The IT Manager will ensure that files are archived onto CD when instructed by the FE. Monthly lists should be available from Accounts to instigate this procedure. FEs should then advise the Accounts Dept or the IT Manager that the file can then be archived on the Case Management system.

## 4.2 Internet and Email Access and Use

The email rules are included at Appendix 19.

## Use of Internet, Intranet and Email Access and Social Media Policy (Appendix 19)

Access to the Internet and email systems is only granted to staff on the basis that they act in a considerate and responsible manner. Access is a privilege, not a right.

1. Employees must not:
   (a) access internet sites or send emails, whether internal or external, containing adult material of a sexual, racial, offensive or pornographic nature under any circumstances;

   (b) use of the internet and/or email services to engage in activities that may be in violation of the law;

   (c) download, load or install any software, unless they have permission from the IT Manager;

   (d) use of the internet and/or email services for personal financial gain, gambling, political, religious or advertising purposes;

   (e) use public chat rooms;

   (f) stay connected to the internet for excessive periods of time;

   (g) send anonymous messages or chain letters via email;

   (h) compromise the security of Business B and its clients;

   (i) use the internet and email services for excessive non-business usage;

   (j) create or transmit any offensive , abusive, obscene or indecent images, data or material;

   (k) create or transmit material which is designed or likely to cause annoyance, inconvenience, embarrassment or needles anxiety;

   (l) create or transmit material of a defamatory nature;

   (m) attempt to monitor, intercept, read or tamper with anyone else's email, unless authorised to do so;

   (n) download any pornographic, defamatory, illegal or inappropriate, such as password cracking software and virus construction kits;

   (o) download any material from untrusted or unknown sources;

(p) use of the internet or email services to place orders or to create liability (financial or otherwise) for Business B or its clients without prior authority;

(q) use profane, abusive, offensive or impolite language in email messages

2. Employees must:

(a) observe and respect copyright and intellectual property rights;

(b) make sure that all emails are sent to the correct recipient;

3. Employees are responsible for the emails they send and for contacts made.

4. Use of the Internet and/or emails services for illegal purposes will be reported to the police;

5. Home Computers and Memory Sticks: You are not allowed to copy documents from the Company's computer network on to personal memory sticks or personal computers without the express consent of a Director on each and every occasion. Memory Sticks given to you by the Company to commemorate the xxth anniversary of the Company are for personal use, and should not be used to take copies from the Company's computer system. Those Directors, Managers and Fee Earners who are authorised to work periodically from should already have been given a direct link to the network server. Any other person must get the express permission of a Director before taking any material in electronic form from the Company's premises.

6. Email and Internet usage is monitored periodically by the Directors and the IT Manager. All emails going in and out of the Company are filtered for spam and personal emails. Such emails are then deleted. All remaining emails are then archived by the IT Manager, burnt to CD and stored in a secure location (Known to the IT Manager) in the event that any email needs to be restored. Archived email CDs will be kept for 7 years, and will then be destroyed.

7. Intranet Site:

There is an Intranet site for use by all employees from within the office. This is available at xxxxxxxx. The Intranet site contains forms and documents

that staff may need in order to fulfil their duties. It also contains news and information of course attended, staff achievements and office social events.

(a) Any documents added to the site are subject to the prior approval of a Director or the FOM, and will then be passed to the IT Manager for inclusion.

(b) Any parts of the site that allow users to add comments etc., users must:
    (i) Not add any material of a sexual, racial, offensive, abusive, impolite, defamatory or pornographic nature, or add material which is likely to cause annoyance, inconvenience, embarrassment or needles anxiety under any circumstance;
    (ii) Observe and respect copyright and intellectual property rights;
    (iii) Not use the Internet for any illegal purposes.

If any user is found to be disregarding the Internet and Email Access and Usage Policy, the Directors reserve the right to disconnect them immediately, and they may be subject to further action under Business B's disciplinary procedures.

## Social Media Policy

### Policy Statement

We recognise that the internet provides unique opportunities to participate in interactive discussions and share information on particular topics using a wide variety of social media, such Facebook, Twitter, blogs and wikis. However, employees' use of social media can pose risks to our confidential proprietary information, and reputation, and can jeopardise our compliance with legal obligations.

To minimise these risks, to avoid loss of productivity and to ensure that out IT resources and communications systems are used only for appropriate business purposes, we expect employees to adhere to this policy.

This policy does not form part of any employee's contract of employment and it may be amended at any time.

### Who is covered by the policy?

This policy covers all individuals working at all levels and grades, including officers, directors, employees, consultants, contractors, trainees, homeworkers, part-time

and fixed-term employees, casual and agency staff (collectively referred to as **staff** in this policy).

Third parties who have access to our electronic communication systems and equipment are also required to comply with this policy.

## Scope and purpose the policy?

This policy deals with the use of all forms of social media, Including Facebook, LinkedIn, Twitter, Wikipedia, all other social networking sites, and all other internet postings, including blogs.

It applies to the use of social media for both business and personal purposes, whether during office hours or otherwise. The policy applies regardless of whether the social media is accessed using out IT facilities and equipment or equipment belonging to members of staff

Breach of this policy may result in disciplinary action up to and including dismissal. Disciplinary action may be taken regardless of whether the breach is committed during working hours, and regardless of whether our equipment or facilities are used for the purpose of committing the breach. Any member of staff suspected of committing a breach of this policy will be required to cooperate with our investigation, which involve handing over relevant passwords and login details.

Staff may be required to remove internet postings which are deemed to constitute a breach of this policy. Failure to comply with such a request may, in itself, result in disciplinary action.

## Personnel responsible for implementing this policy

Our Board of Directors (the Board) has overall responsibility for the effective operation of this policy, but has delegated day-to-day responsibility for its operation to the IT Manager. Responsibility for monitoring and reviewing the operation of this policy and making recommendations for change to minimise risk also lies with the IT Manager.

All Fee Earners have a specific responsibility for operating within the boundaries of this policy, ensuring that all staff understand the standards of behaviour expected of them and taking action when behaviour falls below its requirements.

All staff are responsible for the success of this policy and should ensure that they take the time to read and understand it. Any misuse of social media should be reported to a Director or the IT Manager. Questions regarding the content or application of this policy should be directed to a Director.

For example, employees are prohibited from using social media to:

(a) breach our internet usage and communications policies;
(b) breach our obligations with respect to the rules of relevant regulatory bodies;
(c) breach any obligations they may have relating to confidentiality;
(d) breach our Disciplinary Rules;
(e) defame or disparage the organisation or its affiliates, customers, clients, business partners, suppliers, vendors or other stakeholders;
(f) harass or bully other staff in any way and/or breach our Anti-harassment and Bullying Policy;
(g) unlawfully discriminate against other or third parties and/or breach our Equal Opportunities Policy;
(h) breach our Data Protection Policy (for example, never disclose personal information about a colleague online);
(i) breach any other laws or ethical standards (for example, never use social media in a false or misleading way, such as by claiming to be someone other than yourself or by making misleading statements).

Staff should never provide references for other individuals on social or professional networking sites, as such references – positive and negative – can be attributed to the organisation and create legal liability for both the author of the reference and the organisation.

Employees who breach any of the above policies will be subject to disciplinary action up to and including termination of employment.

## Personal use of Social Media

Personal use of social media is never permitted during working time or by means of our computers, networks and other IT resources and communications systems.

## Monitoring

The contents of our IT resources and communications systems are our property. Therefore, staff should have no expectation of privacy in any message, files, data, document, facsimile, telephone conversation, social media post conversation or message, or any other kind of information or communications transmitted to, received or printed from, or stored or recorded on, our electronic information and communications systems

We reserve the right to monitor, intercept and review, without further notice, staff activities using our IT resources and communications systems, including but not limited to social media postings and activities, to ensure that our rules are being complied with and for legitimate business purposes and you consent to such monitoring by your use of such resources and systems. This might include, without limitation, the monitoring, interception, accessing, recording, disclosing, inspecting,

reviewing, retrieving and printing of transactions, messages, communications, postings, logins, recordings and other uses of the systems as well as keystroke-capturing and other network monitoring technologies.

We may store copies of such data or communications for a period of time after they are created, and may delete such copies from time to time without notice. Do not use our IT resources and communications systems for any matter that you wish to be kept private or confidential from the organisation.

## Business use of Social Media

If your duties require you to speak on behalf of the organisation in a social media environment, you must still seek approval for such communication from a Director, who may require you to undergo training before you do so and impose certain requirements and restrictions with regard to your activities.

Likewise, if you are contacted for comments about the organisation for publication anywhere, including in any social media outlet, direct the enquiry to a Director and do not respond without written approval.

The use of social media for business purposes is subject to the remainder of this policy.

## Recruitment

We may use internet searches to perform due diligence on candidates in the course of recruitment. Where we do this, we will act in accordance with our Data Protection and Equal Opportunities obligations.

## Responsible use of Social Media

The following sections of the policy provide staff with common-sense guidelines and recommendations for using social media responsibly and safely.

Protecting our business reputation:

(a) Staff must not post disparaging or defamatory statements about our organisation, our clients, suppliers and vendors, and other affiliates and stakeholders. And staff should also avoid social media communications that might be misconstrued in a way that could damage our business reputation, even indirectly.
(b) Staff should make clear it clear in social media postings that they are speaking on their own behalf. Write in the first person and use a personal email address when communicating via social media.
(c) Staff are personally responsible for what they communicate in social media. Remember that what you publish might be available to be read by the

masses (including the organisation itself, future employers and social acquaintances) for a long time. Keep this in mind before you post content.

(d) If you disclose your affiliation as an employee of our organisation, you must also state that your views do not represent those of your employer. For example, you could state: "the views in this posting do not represent the views of my employer." You should also ensure that your profile and any content you post are consistent with the professional image that you present to clients and colleagues.

(e) Avoid posting comments about sensitive business-related topics, such as our performance. Even if you make it clear that your views on such topics do not represent those of the organisation, your comments could still damage our reputation.

(f) If you are uncertain or concerned about the appropriateness of any statement or posting, refrain from making the communication until you discuss it with a Director or the IT Manager.

(g) If you see content on social media that disparages or reflects poorly on our organisation or our stakeholders, you should contact the IT Manager or a Director. All staff are responsible for protecting our business reputation.

Respecting intellectual property and confidential information

(a) Staff should not do anything to jeopardise our valuable trade secrets and other confidential information and intellectual property through the use of social media.

(b) In addition, staff should avoid misappropriating or infringing the intellectual property of other companies or individuals, which can create liability for the organisation, as well as the individual author.

(c) Do not use our logos, brand names, slogans or other trademarks, or post any of our confidential or proprietary information without prior written permission.

(d) To protect yourself and the organisation against liability for copyright infringement, where appropriate, reference sources of particular information you post or upload and cite them accurately. If you have any questions about whether a particular post or upload might violate anyone's copyright or trademark, ask the commercial department or a Director before making the communication.

(e) You are not permitted to add business contacts made during the course of your employment to personal social networking accounts, such as Facebook accounts or LinkedIn accounts without the consent of a Director. The contact details of business contacts made during the course of your employment are regarded as our confidential information, and as such you will be required to delete all such details from your personal social

networking accounts, such as Facebook accounts or LinkedIn accounts on termination of employment.

Respecting colleagues, clients, partners and suppliers:

(a) Do not post anything that your colleagues or our customers, clients, business partners, suppliers, vendors or other stakeholders would find offensive, including discriminatory comments, insults or obscenity
(b) Do not post anything related to your colleagues or our customers, clients, business partners, suppliers, vendors or other stakeholders without their written permission.

## Monitoring and review of this policy

The IT Manager, in conjunction the Board, shall be responsible for reviewing this policy annually, to ensure that it meets legal requirements and reflects best practice.

## Appendix B

**Business C's Social Media Policy (extracted from its Staff Handbook).**

## *Social Media*

Policy Statement:

We recognise that the internet provides unique opportunities to participate in interactive discussions and share information on particular topics using a wide variety of social media, such as Facebook, Twitter, blogs and wikis. However, employees' use of social media can pose risks to our confidential and proprietary information, and reputation, and can jeopardise our compliance with legal obligations.

To minimise these risks, to avoid loss of productivity and to ensure that our IT resources and communications systems are used only for appropriate business purposes, we expect employees to adhere to this policy.

## *Who is covered by the policy?*

This policy covers all individuals working at all levels and grades, including senior managers, officers, directors, employees, consultants, contractors, trainees, homeworkers, part-time and fixed-term employees, casual and agency staff [and volunteers] (collectively referred to as staff in this policy).

Scope and purpose of the policy

This policy deals with the use of all forms of social media, including Facebook, LinkedIn, Twitter, Wikipedia, all other social networking sites, and all other internet postings, including blogs.

It applies to the use of social media for business purposes, whether during office hours or otherwise. The policy applies regardless of whether the social media is accessed using our IT facilities and equipment or equipment belonging to members of staff.

Breach of this policy may result in disciplinary action up to and including dismissal. Disciplinary action may be taken regardless of whether the breach is committed during working hours, and regardless of whether our equipment or facilities are used for the purpose of committing the breach. Any member of staff suspected of committing a breach of this policy will be required to cooperate with our investigation, which may involve handing over relevant passwords and login details.

Staff may be required to remove internet postings which are deemed to constitute a breach of this policy. Failure to comply with such a request may, in itself, result in disciplinary action.

Personnel responsible for implementing this policy

The Chief Executive has overall responsibility for the effective operation of this policy. Responsibility for monitoring and reviewing the operation of this policy and making recommendations for change to minimize risks lies with the Chief Executive.

All managers have a specific responsibility for operating within the boundaries of this policy, ensuring that all staff understand the standards of behaviour expected of them and taking action when behaviour fall below its requirements.

All staff are responsible for the success of this policy and should ensure that they take the time to read and understand it. Any misuse of social media should be reported to their manager. Questions regarding the content or application of this policy should be directed to the Chief Executive

Personal use of social media

We recognise that employees may work long hours, and occasionally may desire to use social media for personal activities at the office or by means of our computers, networks and other IT resources and communications systems. We accept such occasional use, as long as it does not involve unprofessional or inappropriate content and does not interfere with your employment responsibilities or productivity. While using social media at work, circulating chain letters or other spam is never permitted. Circulating or posting commercial, personal, religious or political solicitations, or promotion of outside organisations unrelated to the organisation's business are also prohibited. You should make it clear that any views you express, whilst using social

media for personal activities, are your own personal views and not those of Business C.

Monitoring

The contents of our IT resources and communications systems are our property. Therefore, staff should have no expectation of privacy in any message, files, data, document, facsimile, telephone conversation, social media post conversation or message, or any other kind of information or communications transmitted to, received or printed from, or stored or recorded on, our electronic information and communications systems

We reserve the right to monitor, intercept and review, without further notice, staff activities using our IT resources and communications systems, including but not limited to social media postings and activities, to ensure that our rules are being complied with and for legitimate business purposes and you consent to such monitoring by your acknowledgment of this policy and your use of such resources and systems. This might include, without limitation, the monitoring, interception, accessing, recording, disclosing, inspecting, reviewing, retrieving and printing of transactions, messages, communications, postings, logins, recordings and other uses of the systems as well as keystroke-capturing and other network monitoring technologies.

We may store copies of such data or communications for a period of time after they are created, and may delete such copies from time to time without notice. Do not use our IT resources and communications systems for any matter that you wish to be kept private or confidential from the organisation.

Business use of Social Media

If your duties require you to speak on behalf of the organisation in a social media environment, you must still seek approval for such communication from your manager, who may require you to undergo training before you do so and impose certain requirements and restrictions with regard to your activities.

Likewise, if you are contacted for comments about the organisation for publication anywhere, including in any social media outlet, direct the enquiry to your manager and do not respond without written approval.

The use of social media for business purposes is subject to the remainder of this policy.

Recruitment

We may use internet searches to perform due diligence on candidates in the course of recruitment. Where we do this, we will act in accordance with our data protection and equal opportunities obligations.

Responsible use of Social Media

The following sections of the policy provide staff with common-sense guidelines and recommendations for using social media responsibly and safely.

Protecting our reputation:

Our Staff Handbook prohibits staff from posting disparaging or defamatory statements about:

- the organisation,
- its clients,
- suppliers,
- other affiliates and stakeholders,

but staff should also avoid social media communications that might be misconstrued in a way that could damage our business reputation, even indirectly.

Staff should make clear it clear in social media postings that they are speaking on their own behalf. Write in the first person and use a personal email address when communicating via social media. Staff are personally responsible for what they communicate in social media. Remember that what you publish might be available to be read by the masses (including the organisation itself, future employers and social acquaintances) for a long time. Keep this in mind before you post content. If you disclose your affiliation as an employee of our organisation, you must also state that your views do not represent those of your employer. For example, you could state, "the views in this posting do not represent the views of my employer." You should also ensure that your profile and any content you post are consistent with the professional image that you present to clients and colleagues. Avoid posting comments about sensitive business-related topics, such as our performance. Even if

you make it clear that your views on such topics do not represent those of the organisation, your comments could still damage our reputation. If you are uncertain or concerned about the appropriateness of any statement or posting, refrain from making the communication until you discuss it with a Director or the IT Manager.

If you see content on social media that disparages or reflects poorly on Business C, you should contact your manager or the Chief Executive. All staff are responsible for protecting our business reputation.

Respecting colleagues, clients, partners and suppliers:

Do not post anything that your colleagues or our customers, clients, business partners, suppliers, vendors or other stakeholders would find offensive, including discriminatory comments, insults or obscenity.

## Appendix C Business C's ICT Induction Document.

# ICT Induction

## General Introduction to the IT Systems

**Shutting down PC at night**
If you do not take your laptop home, please ensure that you shut it down.

**About the network**
Business C has two servers: an Exchange Server (our main server for emails, document network, tec.) and a Terminal Services Server (which allows for remote access to the network and emails). Further details can be found in the 'Notes on how to use Business C's IT system' document.

**WiFi at Business C**
The WiFi network name is ……. and the password is ……..

**How information is backed up and whose responsibility it is**
All files should be saved to the network in order that they are backed up. The network is backed up offsite.

**PC/Laptop maintenance**
Schedule in your calendar to do the following very month:

1. Double click the desktop icon called "TUNE UP 1-CLICK MAINTENANCE"

2. It will run a five-minute scan and find any issues

3. If it finds problems, a button will appear saying "RUN MAINTENANCE"

4. If the scan has found that the disk is fragmented (last scan item), then the maintenance will take a few hours. If not, click the button and it will resolve all issues in about 30 seconds

5. If the disk is fragmented, then it is recommended that this is done at the end of the day. You can click the "SHUTDOWN PC AFTER MAINTENANCE HAS RUN" button and the start the

maintenance and leave it on. It will automatically shut down the PC/Laptop when completed.

## Username and password

**Your username is xxxxxxxxxxxx**

**What the initial password is and how to change it**
Your initial password is xxxxxxxxxxxx You can change this by pressing Control/Alt/Delete and selecting 'Change Password.' When you have changed your password, please let xxxxxxxxxxxx know what it is.

**Changing your password**
You will be prompted to change your password every 6 months.

**What to do if you forget your password**
Contact xxxxxx Ltd (who manage our IT systems) and they will reset it for you – contact details below.

## Email address info

**Your email address: xxxxxxxxxxxxxxxxxxxx**

## Applications in use

**Office applications**
We use standard Microsoft Office applications – Word, Excel, Powerpoint, etc. If you need any additional training on these, this can be arranged.

**Email, calendaring and contacts software**
Business C uses Outlook. See attached notes. Extra training can be arranged if you require this.

**What to do if you require specialist software**
Please contact xxxxxxxx Ltd. Do not attempt to download any new software programs yourselves.

## What to save and where, permissions on drives and folders

### Drive mappings on the sever and other shared drives

See attached sheet. Please do not save files/folders to the hard drive (C:).

### Where your personal files can be saved

These can be stored on the Z: drive. This is where your should file your timesheets and any other documents which are personal to you.

### Getting set up on website – so you can add, amend, edit backend

Create an account on the website by going to http://xxxxxxxxxxxxxx and complete the details. Once done, please let xxxxxxxxxx know, so that she can do the final set up and explain how to use the backend of the website.

## Data Protection

The following are the Data Protection Principles which Business C seeks to uphold:

- Tell people clearly what the information is needed for and take special care with sensitive information. Be open and fair with people.
- Ensure information is used and disclosed only for the duties for which it was collected.
- Keep only relevant information which is adequate but not excessive for the purpose for which it is held.
- Keep information accurate and up-to-date.
- Hold information only as long as it is necessary for the purpose.
- Allow individuals access to information held on them and amend it where it is not correct.
- Take appropriate security measures to prevent unauthorised or unlawful processing, disclosure, destruction, loss, or alteration of information. Get written confirmation of data protection compliance from suppliers and providers of services.

Please read Business C's Data Protection Policy for further information.

## Help and Support

### Internal support staff

xxxxxxx xxxxxxx – Office Manager – for any minor IT queries.

**Liaison with external support and how to contact them**
We have a full maintenance support contract with xxxxxxxxxx Ltd, and It company based in xxxxxxxxxxxx. They can be contacted on xxxxxxxxx or xxxxxxxxx – ask to speak to X, Y or Z. Alternatively, you can email support@xxxxxxxxxxxxxxx They are happy for staff to contact them with any queries.

**What to do if you suspect you have been sent a virus**
Forward to support@xxxxxxxxxxxxxx Do not open any attachments.

## Appendix D 'Notes on how to use Business C's IT system' Document.

# Notes on how to use Business C's IT system

### Accessing the network

Go to 'my computer,' then:

- S: drive for xxx Work, Scans folder.
- V: drive for archive.
- Z: drive for 'my documents'/home.
- We can log on to our desktops from any machine in the building (plus see next section about remote working).
- We need to keep our laptops as 'clean' as possible. Therefore, don't save documents or folders to the desktop (unless on a very temporary basis) and instead save them in xxxx Work or My Documents. You can keep shortcuts to documents on your desktop though.
- **Empty the 'recycle bin' on your desktop regularly.**
- If you want new software installed, please contact xxxxxxxxx LTs (the IT Support company), don't install yourself.
- Smartphones can be synchronised to access emails, calendars, contacts, etc. – please contact xxxxxxx Ltd.
- The AVG (anti-virus scan) is scheduled to run on Wednesdays at noon. Whilst it is running, you can still work but the system will run slower. You can change when you want your scheduled scan to run by clicking on the AVG icon on your desktop, then click on scan options and then on manage scheduled scans. It needs to run every week.

### Accessing the xxx server remotely (the main and best way for remote access)

- Save 'remote to server' attachment to your desktop. You can also put it on a memory stick if you want. (if using a ac, you'll need to download some RDP software first – probably best to ask xxxxxxx (the IT Support company) about this if not sure!).
- Log on with username as xxxxxxx\firstname.lastname and your password.
- Click yes when security warning message comes up.
- Your desktop should then magically appear, and once you are logged on you can work as normal.
- Only 10 people can be logged on remotely at any one time. If an 11th person tries, they will get an error message come up. Whilst it is unlikely that that many people will be working remotely at any one time, if you are stopping work for any length of time,

please remember to log out, to leave space for other people. If the server detects that you have not been working for a certain length of time anyway, it will first warn you and then log you out, so remember to save all your work frequently otherwise you will lose it.

- If you want to print to your home computer from the network, please send xxxxxxxx (the IT support company) the make/model of your printer.

**Remote web access (use as emergency/last resort – e.g. if you don't have access to the above remote login)**

- Enter https://remote.xxxxxxxxxxxxx as the url in your web browser.
- Put your username as firstname.lastname and your password.
- You can then access your emails, shared folders and home folders (although everyone's names are listed under home folder, you can only open your own).
- If you want to work on a particular document, download it to your local machine and then, when finished, upload it back onto the server. You can also download a whole folder if you want. Just tick next to the folder you want and click on the download button in the menu bar above – then save to where you want it. When you have finished, do the same and click upload.

**Using Microsoft Outlook**

Some useful pointers. You can also get helpful short tutorials on Outlook in YouTube. Please also note the things we need to do (in bold):

**Emailing:**

- You can edit your signature by going to Tools – options – mail format – click on signatures box. You can also set up new signatures. To remove double spacing between lines, press shift-enter then delete. To change which signature you use in email, right click on the current email and select the one you wish to use.
- Do not use auto archive facility. To stop prompts popping up: Go to Tools menu and then go to Options, select Other tab on the window that comes up, and then click Auto Archive button, then uncheck the top 2 options and it will stop the reminders and the prompts.

- **Make sure you delete emails that you no longer need, especially those with large attachments, as our emails are all part of the offsite backup system.**

**Calendar:**

- **You need to set your permission level to allow other staff to view your calendar.** Click on 'share my calendar' in left-hand pane of calendar view, select who you want to view your calendar and then choose the permission level – if you click on the different options (e.g. 'reviewer') you can see what boxes get ticked.
- To view other staff calendars, go to 'Open Calendar,' 'From Address Book,' 'All Staff.'

**Dealing with Spam**

Use the 'Junk' button in Outlook to deal with spam emails which come into your inbox, and legitimate emails which go into your junk.

**You need to go through your junk mail box regularly and delete. The more you use the spam filter, the less 'legitimate' mail will be in your junk mailbox. Also, remember to empty your 'deleted' folder regularly.**

**Dealing with spam emails**

- Don't open any suspicious attachments. xxxxx (the IT Support company) has put a stop on us opening zip folders, as these are the main culprit. If you know that someone legitimate wants to send you a zip file, please let me know. Apparently, it is opening suspicious attachments, rather than the actual email, which is the problem.
- Use your 'This is spam' and 'This is legitimate mail' folders. If you don't know how to do this, or what these folders are, please let me know
- Remember to empty your deleted mail box regularly.
- Always fill in a subject heading when sending an email.
- Even if an email is marked 'Internal,' it won't be – the spammers do this to try to fool people.
- If an email in your Junk box looks like it is from a member of staff, it won't be.
- Always use your full email signature, even in internal emails.
- Don't click on suspicious links.

# Appendix E

**Listing of the thematic framework used in the Documentary Analysis.**

Matrices

**1 Responsibility**

1.1 Individual

1.2 Corporate

1.3 Governmental

1.4 Shared

**2 Knowledge and Behaviour**

2.1 Awareness

2.2 Education

2.3 Advice

2.4 Practices

Headings (for more specific categorisation within those Matrices)

Compliance
*Cyber Essentials*
Cyber Insurance
*Cyber Streetwise*
Managing User Privileges
Monitoring User Behaviour
Mobile
Prevention
Shaping Victim Status
Social Engineering
Social Networking

## Appendix F List of the twenty-five documents analysed during the Documentary Analysis.


Cabinet Office (2011) *The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world*. HMSO. Available from: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf [accessed 17 September 2014].

Cabinet Office (2014) *The UK Cyber Security Strategy Report on Progress and Forward Plans: December 2014.* HMSO. Available from: https://www.gov.uk/government/publications/national-cyber-security-strategy-2014-progress-and-forward-plans [accessed 21 December 2015]

Cabinet Office (2015) Cyber insurance joint statement, 5 November 2015. HMSO. Available from: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/371036/Cyber_Insurance_Joint_Statement_5_November_2014.pdf [accessed 6 November 2015].

Cabinet Office (2015a) *UK Cyber Security: The role of insurance in managing and mitigating risk*. HMSO. Available from: https://www.gov.uk/government/publications/uk-cyber-security-the-role-of-insurance [accessed 3 June 2016].

Cabinet Office (2015b) *Cyber security insurance: New steps to make UK world centre*, Press Release, 23 March 2015. Available from: https://www.gov.uk/government/news/cyber-security-insurance-new-steps-to-make-uk-world-centre [accessed 3 June 2016].

Cabinet Office (2015c) *10 Steps to Cyber Security: Executive Companion*. HMSO. Available from: https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility/10-steps-executive-companion [accessed 9 July 2016).

Department for Business, Innovation & Skills (2014) *Cyber Essentials Scheme: Requirements for basic protection from cyber attacks*. HMSO. Available from:

https://www.gov.uk/government/publications/cyber-essentials-scheme-overview [accessed 3 June 2016].

Department for Business, Innovation & Skills (2014a) *2014 Information Security Breaches Survey*. HMSO. Available from: https://www.gov.uk/government/publications/information-security-breaches-survey-2014 [accessed 17 September 2014].

Department for Business, Innovation & Skills (DBIS) (2014b) *Cyber Essentials Scheme: Summary*. HMSO. Available from: https://www.gov.uk/government/publications/cyber-essentials-scheme-overview [accessed 3 June 2016].

Department for Business, Innovation & Skills (2015) *Small businesses: What you need to know about cyber security*, March 2015. Available from: https://www.gov.uk/government/publications/cyber-security-what-small-businesses-need-to-know [accessed 21 December 2015].

Department for Business, Innovation & Skills (2015a) *2015 Information Security Breaches Survey*. HMSO. Available from: https://www.gov.uk/government/publications/information-security-breaches-survey-2015 [accessed 31 December 2015].

Department for Culture, Media and Sport (2015), *UK businesses urged to protect themselves from growing cyber threat*, Press Release, 22 September 2015. Available from: https://www.gov.uk/government/news/uk-businesses-urged-to-protect-themselves-from-growing-cyber-threat [accessed 21 December 2015].

Department for Culture, Media and Sport (2015a), Digital Economy Minister (Ed Vaisey MP), *Speech on the Government's work with UK businesses on cyber security*, Internet Security Summit, London, 18 November 2015. Available from: https://www.gov.uk/government/speeches/digital-economy-ministers-speech-on-cyber-security-for-uk-businesses [accessed 21 December 2015].

Department for Culture, Media and Sport (2016), Minister for Digital and Culture Minister (Matthew Hancock MP), *Speech addressing the CBI*, 2nd Annual CBI Cyber Security Conference, London, 14 September 2016. Available from:

https://www.gov.uk/government/speeches/minister-for-digital-and-culture-addresses-cbi-conference [accessed 15 September 2016].

Federation of Small Businesses (2013) *Cyber Security and fraud: The impact on small businesses*. Available from: http://www.fsb.org.uk/docs/default-source/Publications/reports/fsb_cyber_security_and_fraud_paper_final.pdf?sfvrsn=0 [accessed 3 June 2016].

Federation of Small Businesses (2015) *Cyber Security and fraud: The impact on small businesses*, Press Release, Tuesday 1 September 2015. Available from http://www.fsb.org.uk/media-centre/latest-news/2015/09/24/cyber-security-and-fraud-the-impact-on-small-businesses [accessed 31 December 2015].

GCHQ (2013) *Countering the cyber threat to business* (including the *10 Steps to Cyber Security*). In Institute of Directors, *Big Picture*. Available from: https://www.gchq.gov.uk/countering-cyber-threats-business [accessed 17 September 2014].

HM Treasury (2015) *Chancellor's speech to GCHQ on cyber security* (as part of the Spending Review and Autumn Statement 2015), 17 November 2015. Available from: https://www.gov.uk/government/speeches/chancellors-speech-to-gchq-on-cyber-security [accessed 29 December 2015].

Home Office (2013) *Cyber Crime: A review of the evidence*. Home Office Research Report 75. HMSO. Available from: https://www.gov.uk/government/publications/cyber-crime-a-review-of-the-evidence [accessed 17 September 2014].

Home Office (2014) *Cyber Streetwise*. Available from: https://www.cyberstreetwise.com/ [accessed 17 September 2014].

House of Commons Science and Technology Committee (2012) *Malware and cyber crime*. HMSO. Available from: http://www.parliament.uk/business/committees/committees-a-z/commons-select/science-and-technology-committee/inquiries/parliament-2010/malware-and-cyber-crime/ [accessed 17 September 2014].

House of Commons Home Affairs Committee (2013) *Report on E-Crime*. HMSO. Available from: http://www.publications.parliament.uk/pa/cm201314/cmselect/cmhaff/70/70.pdf [accessed 17 September 2014].

House of Commons Culture, Media and Sport Committee (2016) *Cyber Security: Protection of Personal Data Online*. Available from: http://www.parliament.uk/business/committees/committees-a-z/commons-select/culture-media-and-sport-committee/inquiries/parliament-2015/cyber-security-15-16/ [accessed 18 July 2016].

House of Lords Science and Technology Committee (2007) *Report on Personal Internet Security*. HMSO. Available from: http://www.publications.parliament.uk/pa/ld200607/ldselect/ldsctech/165/165i.pdf [accessed 29 December 2015].

Symantec (2015) *Internet Security Threat Report*, Volume 20, April 2015. Available from: http://www.symantec.com/security_response/publications/threatreport.jsp [accessed 31 December 2015].

# Appendix G The data from the Documentary Analysis set within the thematic framework.

### 1. Framework matrix for the theme: 'Responsibility'

| Source | 1.1 Individual | 1.2 Corporate | 1.3 Gov'tal | 1.4 Shared |
|---|---|---|---|---|
| Cabinet Office (2011) | Ordinary people have an important role to play in keeping cyberspace as a safe place to do business and live our lives.<br><br><u>Shaping Victim Status</u><br>[By 2015, we want a UK where:] People are clear that, as in the offline world, we are each responsible for our behaviour in cyberspace. | [By 2015, we want a UK where:] The private sector has a crucial role to play in the UK's cyber security.<br><br>Much of cyberspace is owned and used by private companies. It is businesses that will drive the innovation required to keep pace with security challenges.<br><br>Ultimately, it is the private sector that owns the assets and makes the business decisions about investing in cyber security.<br><br><u>Prevention</u><br>Through their relationship with their customers, ISPs can make an important contribution to identifying and preventing cyber attacks on UK networks. | | Achieving this vision will require everybody, the private sector, individuals and government to work together.<br><br>Though the scale of the challenge requires strong national leadership, Government cannot act alone.<br><br>Outreach to business and the public is crucial.<br><br>With the rise of cybercrime, what was a concern primarily for the defence and intelligence elements of government is now something that concerns all of us.<br><br>We are clear that the debate must involve all those with a stake in an open, trusted and stable cyberspace, including industry, business and representatives of civil society.<br><br>The need for us all to work collectively to tackle the threat from criminals acting online.<br><br>As with most change, increasing our reliance on cyberspace brings new opportunities but also new threats.<br><br>While cyberspace fosters open markets |

| | | | | |
|---|---|---|---|---|
| | | | | and open societies, this very openness can also make us vulnerable to those – criminals, hackers, foreign intelligence services – who want to harm us by compromising or damaging our critical data systems.<br><br>Business is the largest victim of crime and economic espionage perpetrated through cyberspace. Responsibility for the issue must be shared by government and the private sector.<br><br><u>Prevention</u><br>[By 2015 we want a UK where] Private organisations work in partnerships with each other, government and law enforcement agencies, sharing information and resources, to transform the response to a common challenge, and actively deter threats that we face in cyberspace. |
| Cabinet Office (2014) | | <u>Cyber Essentials</u><br>In June 2014, GCHQ, BIS and the Cabinet Office launched Cyber Essentials, a major new Government-backed and industry supported scheme to incentivise widespread adoption of basic security controls that will help to protect organisations against the commonest kinds of internet attacks. | | |
| Cabinet Office (2015) | | <u>Cyber Insurance and Prevention</u><br>The government supports the growth of the cyber insurance market to | | <u>Cyber Insurance and Prevention</u><br>Partnership between government and industry is crucial, and this event [the |

| | | | | |
|---|---|---|---|---|
| | | improve how UK businesses manage cyber security risk.<br><br>The government believes that cyber insurance has a strong role to play in helping firms outside of the critical national infrastructure to manage their cyber risks efficiently.<br><br>Cyber insurance does not, of course, remove the need for businesses to manage their risk from cyber attack. It should be seen as part of an holistic approach to cyber risk management, including business controls, investment in security and education of staff and customers. | | working groups report on cyber insurance] is the next step in an ongoing partnership to address cyber threats to UK businesses and to wider UK interests. |
| Cabinet Office (2015a) | | <u>Shaping Victim Status</u><br>[There is a] need to move away from treating cyber primarily as a technology or security issue, to one that is owned collectively as a key risk to firm viability and that permeates the way the business is run.<br><br><u>Cyber Insurance and Shaping Victim Status</u><br>The [cyber insurance] Report includes some important messages for business. One is the need to value the risk of cyber attack properly.<br><br>[The Report] also shows that many businesses are overestimating the extent to which their existing insurance | | There is a tendency to think of cyber as a new, and hence unique, threat. In fact, many aspects of it – the risk of business interruption, the potential for large and public impact, and the need for rapid response post-event – are common to other tail risks (low frequency, high impact events), such as natural catastrophe and terrorism. |

| | | | | |
|---|---|---|---|---|
| | | provides cover for cyber risk.<br><br>Another clear conclusion is that some businesses still feel that they do not fully understand the risk of cyber attack properly. This highlights the need for companies to have clear accountability structures for cyber risk, and to put in place robust cyber security risk management arrangements. | | |
| Cabinet Office (2015b) | | <u>Prevention and Shaping Victim Status</u><br>Companies are recommended to stop viewing cyber largely as an IT issue, and focus on it as a key commercial risk affecting all parts of its operations.<br><br><u>Cyber Insurance and Shaping Victim Status</u><br>Insurance is not a substitute for good cyber security, but is an important addition to a company's overall risk management.<br><br><u>Cyber Insurance, Cyber Essentials and Shaping Victim Status</u><br>Insurers' support shows the success of the Cyber Essentials scheme. They recognise that having Cyber Essentials certification is a valuable indicator of a mature approach to cyber security in SMEs that contributes to the reduction of risk. | | |

| | | | | |
|---|---|---|---|---|
| | | Cyber Insurance<br>Marsh will launch a new cyber insurance product for SMEs which will absorb the cost of Cyber Essentials certification for the majority of firms, which the government encourages other [insurance] brokers to follow. | | |
| Department for Business, Innovation & Skills (2014) | | Shaping Victim Status<br>Regardless of their size, use of technology, the industry sector in which they operate and their global presence, every organisation needs to implement a robust and effective approach to cyber security. | | |
| Department for Business, Innovation & Skills (2015) | | If you fall victim to online fraud or attack, you should report the incident to the police via the Action Fraud website. You may need to notify your customers and suppliers if their data has been compromised or lost.<br><br>Prevention<br>You can never be totally safe, but most online attacks can be prevented or detected with basic security practices for your staff, processes and IT systems.<br><br>Ensure that your staff have appropriate training, so that everyone understands their role in keeping the business secure.<br><br>Prevention<br>Make your staff aware of cyber security threats and | | |

| | | | | |
|---|---|---|---|---|
| | | how to deal with them.<br><br><u>Managing User Privileges</u><br>Restrict staff and third party access to IT equipment, systems and information to the minimum required.<br><br><u>Monitoring User Behaviour</u><br>Monitor use of all equipment and IT systems, collect activity logs, and ensure that you have the capability to identify any unauthorised or malicious activity. | | |
| Department for Business, Innovation & Skills (2015a) | <u>Shaping Victim Status</u><br>Despite the increase in staff awareness training, people are as likely to cause a breach as viruses and other types of malicious software.<br><br><u>Shaping Victim Status</u><br>People are the main vulnerabilities to a secure enterprise. [Survey] Respondents believe that inadvertent human error (48%), lack of staff awareness (33%) and weaknesses in vetting individuals (17%) were all contributing factors in causing the single worst breach that | <u>Cyber Essentials and Shaping Victim Status</u><br>All businesses and organisations should adopt the [Cyber Essentials] scheme as a vital first step – no ifs or buts.<br>Of course, many businesses and organisations will need to have in place far more controls and procedures to manage the risks they face, and we will continue to work with them to make this happen.<br><br><u>Monitoring User Behaviour and Shaping Victim Status</u><br>When questioned about the single worst [information security] breach suffered, 50% of the organisations [which responded to the survey] attributed the cause to inadvertent human error (up from 31% in 2014). | | |

| | | | | |
|---|---|---|---|---|
| | organisations suffered.<br><br><u>Shaping Victim Status</u><br>Breaches are increasingly due to people within an organisation – often inadvertently. | <u>Shaping Victim Status</u><br>72% of the companies [surveyed] in which the security policy was poorly understood had staff-related breaches.<br><br><u>Prevention and Shaping Victim Status</u><br>The nature of the most serious incidents is changing to become more targeted; small businesses should not presume that they will escape targeted attacks. All businesses should ensure that they understand their information assets, and manage the risk to them accordingly.<br><br><u>Shaping Victim Status</u><br>Breaches are increasingly due to people within an organisation – often inadvertently. Whilst technical controls have their place, organisations should take the opportunity to question the balance between their investment in technical controls and measures to address human factors.<br><br><u>Shaping Victim Status</u><br>It is notable that there has been a lack of progress amongst small organisations in developing information security policies. Since 2012, there has been little change in the percentage of small organisations [surveyed] who have | | |

| | | | | |
|---|---|---|---|---|
| | | formally documented an information security policy, but the trend in those organisations suffering a breach has increased over the same time.<br><br><u>Cyber Insurance</u><br>The impending revision of the EU Data Protection Regulation is expected to include mandatory notification of breaches of personal data, and this may well be the catalyst to change the cyber liability insurance landscape in the UK. | | |
| Department for Culture, Media & Sport (2015) | | Trust and confidence in UK online security is crucial for consumers, business and investors.<br><br><u>Cyber Essentials</u><br>We want to make the UK the safest place in the world to do business online, and Cyber Essentials is a great and simple way that firm can protect themselves. | | We need [good cyber security] to keep our businesses, citizens and public services safe. The UK is a world leader in the use of digital technologies, but we also need to be a world leader in cyber security. |
| Department for Culture, Media & Sport (2015a) | | Working with industry, we have started to transform business understanding and response, by getting cyber security out of the IT department and into the boardroom.<br><br>There has been a great deal of Parliamentary and media interest since the attack on Talk Talk [last month – Oct 2015]…I believe that we need we need to take this moment as a timely reminder that we need to take action | The Chancellor made a major speech yesterday [17 Nov 2015], in which he announced Government plans to invest £1.9 billion in cyber security over the next five years. This more than doubles the current level of Government investment, something which is absolutely necessary if we are to make Britain the best protected | We need to keep our businesses, citizens and public services safe.<br><br>There's been a great deal of parliamentary and media interest since the attack on Talk Talk. No one likes to see the theft of data. But I believe we need to take this moment as a timely reminder that we need to take action to protect ourselves. I hope that businesses around the country are taking the opportunity to |

| | | | | |
|---|---|---|---|---|
| | | to protect ourselves. I hope that businesses around the country are taking the opportunity to review how they deal with cyber security.<br><br><u>Cyber Essentials</u><br>If you adopt Cyber Essentials in your business, you will protect your business against the majority of threats on the internet. | country in cyberspace. | review how they deal with cyber security. |
| Department for Culture, Media & Sport (2016) | | <u>Cyber Essentials and Shaping Victim Status</u><br>I think that every organisation which which relies on the Internet for business should have Cyber Essentials as a minimum.<br><br>Every company in your supply chain that adopts Cyber Essentials, in turn increases your security. | | |
| Federation of Small Businesses (2013) | | Fraud and online crime is a barrier to growth for small and micro businesses. It prevents some businesses from online trading because of the fear or actual risk of fraud. This is particularly concerning given that the Government is looking towards small businesses for economic growth and to create jobs.<br><br><u>Prevention and Shaping Victim Status</u><br>Cyber security is a crucial part of the Government's National Cyber Security Strategy, and we need to make sure that all businesses, large and | | |

| | | | | |
|---|---|---|---|---|
| | | small, are engaged in implementing appropriate prevention measures.<br><br><u>Shaping Victim Status</u><br>Alongside the action that Government and the public sector need to take, businesses need to help themselves more. | | |
| Federation of Small Businesses (2015) | | <u>Shaping Victim Status</u><br>Too many firms ignore the threat of cybercrime.<br><br><u>Shaping Victim Status</u><br>Many businesses simply don't realise that they are at risk, and often assume that cyber criminals are only targeting banks or larger online retailers.<br><br><u>Shaping Victim Status</u><br>Online crime and fraud is a growing and a real threat for small businesses. It is a continually mutating challenge, and businesses need to be live to the many different types of frauds to which they may be victim……The fact that each small business loses up to £4,000 per year to [it] should be a wake-up call also to those who have not so far implemented protections in their business. | | |
| GCHQ (2013) | <u>Compliance and Shaping Victim Status</u><br>Without exception, all users should be | <u>Managing user Privileges</u><br>All users should only be provided with the privileges they need to do their job. | The buck has to stop somewhere, and ultimately it is down to the legislator to | Cyber security is not just an issue for governments – it's for companies and citizens too. |

| | | | | |
|---|---|---|---|---|
| | aware of….their responsibility to adhere to security policies.<br><br>New users (including contractors and third party users) [should be made] aware of their personal responsibility to comply with… security policies.<br><br><u>Shaping Victim Status</u> All users have a responsibility to manage the risks to ICT and information assets. | <br><br><u>Compliance</u><br>Establish a staff induction process [to inform new users of their personal compliance responsibilities].<br><br><u>Compliance</u><br>'Employees' use of ICT brings risks, so it is critical for all staff to be aware of their personal security responsibilities.<br><br><u>Shaping Victim Status</u><br>Establish a formal disciplinary process, making staff aware that any abuse of security policy will result in disciplinary action. | decide where the buck should stop. | |
| HM Treasury (2015) | Citizens need to follow basic rules of keeping themselves safe – installing security software, downloading software updates, using strong passwords. | Companies need to protect their own networks, and harden themselves against cyber attack.<br><br>Of course, our involvement with industry on cyber goes well beyond the cyber sector. We need to make sure that Britain has the regulatory framework it needs, particularly in the sectors we define as the Critical National Infrastructure…So, government has a responsibility towards these sectors, and the companies in those sectors have a responsibility to ensure their own resilience.<br><br>We will work with businesses across the economy to ensure that they have the right defences in place. | In 2010, at a time when we as a new government were taking the most difficult decisions on spending in other areas, we took a deliberate decision to increase spending on cyber. We set up the National Cyber Security Programme and funded it with £860 million…In the [2015] Spending Review, I have made a provision to almost double our investment to protect Britain from cyber attack and develop our sovereign capabilities, totalling £1.9 billion over five years.<br><br>We will be boosting the capabilities of the National Cyber | For our country, defending our citizens from hostile powers, criminals or terrorists, the internet represents a critical axis of vulnerability.<br><br>We need to make sure that Britain has the regulatory framework it needs, particularly in the sectors we define as the Critical National Infrastructure |

| | | | | |
|---|---|---|---|---|
| | | | Crime Unit, so that – in partnership with their counterparts around the world – they attack the assumption among too many that cyber crime is risk free, and comes with little risk of consequences.<br><br>For our country, defending citizens from hostile powers, criminal or terrorists, the internet represents a critical axis of potential vulnerability.<br><br>Government has a unique ability to aggregate and educate. Government has a duty to protect the country from cyber attack, and to ensure that the UK can defend itself in cyberspace. | |
| Home Office (2014) | | <u>Shaping Victim Status</u><br>Ensure that you have good staff policies in place, as these outline for your staff what is expected of them in relation to online security.<br><br><u>Managing User Privileges</u><br>It is best practice to restrict as many permissions as possible, so that staff only have access to information and parts of the IT systems that they need. | | |
| HoC Science and Technology | | <u>Shaping Victim Status</u><br>Good advice is provided on banking | We believe the Government has a duty to protect the people of the | |

| | | | | |
|---|---|---|---|---|
| Committee (2012) | | sites, but you get the feeling that the banks are trying to minimise their responsibilities in these areas [Prof. Sommer]. | United Kingdom from crime, regardless of whether that crime takes place on the streets or on the Internet. | |
| HoC Home Affairs Committee (2013) | | <u>Shaping Victim Status</u><br>[Regarding internet banking fraud] The banks certainly claim that they will blame people if there was gross negligence. In practice, they often blame people as a routine matter, even when then it is not clear there was negligence at all……Everybody is trying to push liability on everybody else. It is even fashionable in the industry. We call it leverage [Prof. Anderson].<br><br><u>Monitoring User Behaviour and Shaping Victim Status</u><br>[Symantec] has said that software providers would only accept liability for their products if they could assume a level of control over the way in which they were being used. | | |
| HoC Culture, Media and Sport Committee (2016) | | [Re. the Talk Talk hack in October 2015] It is no longer a defence for a company using an e-commerce platform to say that it was not aware of the risk of SQL injection-based attacks, or…[similar] forms of cyber-penetration. | | |
| HoL Science and Technology Committee (2007) | <u>Shaping Victim Status</u><br>The current emphasis of Government and policy makers upon end user responsibility | The IT industry and businesses operating online should take their share of responsibility for reducing risk…Even risks arising from carelessness, which | | |

| | | | | |
|---|---|---|---|---|
| | bears little relation either to the capabilities of many individuals or to the changing nature of the technology and the risk.<br><br><u>Prevention</u><br>There are two key aspects to improving the ability of individuals to manage online security. One is to promote awareness of the risks online; the second is to instil knowledge of how practically to manage them. Both are necessary – one without the other is of little use. | might seem to be a purely individual responsibility, could be mitigated if software products were designed with detection tools that could spot and alert users to characteristic acts of carelessness, such as disclosure of personal information without adequate security. The key [is] that products should be developed in such a way as to educate consumers about risks and to provide them with the tools to manage these risks. | | |
| Symantec (2015) | <u>Mobile and Shaping Victim Status</u><br>[Last year] Mobile was also ripe for attack, as many people only associate cyber threats with their PCs and neglect even basic security precautions on their smartphones. In 2014, Symantec found that 17 percent of Android apps (nearly one million in total) were actually malware in disguise. | <u>Social Engineering</u><br>Savvy attackers are using increased levels of deceptions and, in some cases, hijacking companies' own infrastructure and turning it against them. In 2014, Symantec observed advanced attackers, inter alia, using stolen email accounts from one corporate victim to spear phish their next corporate victim, and hiding inside software vendors' updates, in essence 'Trojanizing' updates, to trick targeted companies into infecting themselves…….Given all of this stealthy activity……Almost no company, | | |

| | | | | |
|---|---|---|---|---|
| | | whether large or small, is immune.<br><br><u>Social Media, Social Engineering and Shaping Victim Status</u><br>Email remains a significant attack vector for cybercriminals, but there is a clear movement toward social media platforms. Social media scams spread rapidly and are lucrative for cybercriminals because people are more likely to click something posted by a friend. | | |

**2. Framework matrix for the theme: 'Knowledge and Behaviour'**

| Source | 2.1 Awareness | 2.2 Education | 2.3 Advice | 2.4 Practices |
|---|---|---|---|---|
| Cabinet Office (2011) | [By 2015, we want a UK where:] Everyone, at home and at work, can help identify threats in cyberspace and report them.<br><br>Organisations are not always aware of the new vulnerabilities that dependence on cyberspace can bring.<br><br>As well as working with consumers, we need to raise awareness in business of the potential threat to reputation, revenues and intellectual property from cyber attack.<br><br><u>Prevention</u><br>[We need to] Raise awareness | [By 2015, we want a UK where:] People know how to get themselves a basic level of protection against threats online.<br><br>[In order to help people protect themselves, we will:] Look at the best ways to improve cyber security education at all levels, so that people are better equipped to use cyberspace safely.<br><br>Some sectors of the economy, particularly small and medium sized businesses, do not have access to the skills and knowledge to protect themselves online.<br><br><u>Prevention</u> | We recognise that there are challenges in ensuring that the public has access to the information and skills they require to understand the threat and take actions to operate safely online.<br><br>Although government already provides advice to organisations that run our infrastructure, on how to manage the risks in cyberspace, the adoption of this approach needs to be broader.<br><br><u>Prevention</u><br>[By 2015, we want a UK where:] People have access to accurate | <u>Prevention</u><br>Prevention is key. Most common cyber incidents could be prevented by quite simple 'cyber hygiene.'<br><br><u>Shaping Victim Status</u><br>80% or more of currently successful attacks exploit weakness that can be avoided by following simple best practice, such as updating anti-malware software regularly.<br><br>The joint public/private sector has a key role to play in helping to identify and manage threats by sharing information.<br><br>A joint public/private sector |

| | | | | |
|---|---|---|---|---|
| | amongst businesses of the threat and actions that they can take to protect themselves, including working through strategically important sectors to raise cyber security issues throughout their supply chains. | Because prevention is key, we will work to raise awareness and to educate and empower people and firms to protect themselves online. | and up-to-date information on the online threats that they face, and the techniques and practices they can employ to guard against them. | 'hub' will pool government and private threat information and pass that out to 'nodes' in key business sectors, helping them identify what needs to be done, and providing a network for sharing best practice. |
| Cabinet Office (2014) | <u>Cyber Essentials</u><br>In June 2014, GCHQ, BIS and the Cabinet Office launched Cyber Essentials, major new Government-backed and industry supported scheme to incentivise widespread adoption of basic security controls that will help to protect organisations against the commonest kinds of internet attacks.<br><br><u>Cyber Streetwise</u><br>Cyber Streetwise launched in January 2014, with the goal of measurably improving cyber security amongst the public and small and medium sized businesses. | | | |
| Cabinet Office (2015) | | | | <u>Cyber Insurance and Prevention</u><br>Cyber insurance does not, of course, remove the need for businesses to manage their risk from cyber attack. It should be seen as part of an holistic approach to cyber risk management, including business controls, investment in security and education of staff and customers. |

| | | | | |
|---|---|---|---|---|
| Cabinet Office (2015a) | <u>Prevention and Cyber Essentials</u><br>Recent government research [conducted by the Cyber Streetwise campaign] found that 22% of small businesses admit that they 'don't know where to begin' with cyber security, demonstrating the importance of the government's recently launched Cyber Essentials scheme.<br><br><u>Cyber Insurance</u><br>Insurance is not currently seen as relevant to cyber resilience. Indicatively, half of firm leaders we spoke to do not realise that cyber risks can even be insured. | | | |
| Cabinet Office (2015b) | <u>Cyber Insurance and Shaping Victim Status</u><br>The [cyber insurance] report also notes a significant gap in awareness around the use of insurance, with around half about half of the firms interviewed being unaware that insurance was available for cyber risk. Other surveys suggest that, despite the growing concern among UK companies about the threat of cyber attacks, less than 10% of UK companies have cyber insurance protection, even though 52% of CEOs believe that their companies | | | <u>Cyber Insurance and Cyber Essentials</u><br>In particular, [the cyber insurance report] highlights the exposure of firms to cyber attacks among their suppliers, with a key a agreement that participating insurers will include the government's Cyber Essentials certification as part of their risk assessment for small and medium-sized businesses.<br><br><u>Prevention, Cyber insurance and Cyber Essentials</u><br>Participating insurers will include Cyber Essentials as part of their cyber risk assessment for SMEs when backed by a suitable insurance policy in |

| | | | | |
|---|---|---|---|---|
| | have some form of coverage in place. | | | order to improve their supply chain resilience. This will simplify the application process for business. |
| Department for Business, Innovation & Skills (2014) | Large organisations would already be expected to have some knowledge or experience of cyber security. However, like smaller companies, many still have limited capability to implement the full range of controls necessary to achieve robust cyber protection. | | Small organisations (including single employee businesses), and even some medium-sized organisations, may need to obtain further guidance and support to ensure the technical controls [presented in this Cyber Essentials scheme] can be implemented adequately. | |
| Department for Business, Innovation & Skills (2014a) | Many businesses are becoming more aware of the importance of education on security.<br>As organisations improve their understanding of the security threats they face, they are doing more to manage the associated threats they face. | <u>Shaping Victim Status</u><br>More organisations are explaining their security risks to their staff to ensure that they take the right actions to protect the information. However, this is not universal. | | [Organisations] are doing more to manage the associated risks and seeking new ways to gain assurance over security.<br><br>Organisations are making risk-based decisions about the introduction of mobile devices in order to facilitate more flexible ways of working'<br><br>69% of respondents currently invest in, or plan to invest in, threat intelligence. |
| Department for Business, Innovation & Skills (2015) | <u>Prevention</u><br>Make your staff aware of cyber security threats and how to deal with them. | <u>Prevention</u><br>Ensure that your staff have appropriate training, so that everyone understands their role in keeping the business secure. | | <u>Prevention</u><br>Restrict the use of removable media such as USB drives, CDs, DVDs and secure digital cards, and protect any data stored on such media to prevent data being lost and malware from being installed.<br><br><u>Managing User Privileges</u><br>Ensure that sensitive data is encrypted |

| | | | | |
|---|---|---|---|---|
| | | | | when stored or transmitted online, so that data can only be accessed by authorised users. |
| Department for Business, Innovation & Skills (2015a) | <u>Shaping Victim Status</u><br>There is a noticeable increase of 37% of staff-related breaches in [the surveyed] organisations where security policy was meant to be understood. | | | <u>Cyber Insurance</u><br>[Only] 39% of the large organisations and 27% of the small organisations surveyed have insurance that would cover them in the event of a breach [down 13% and 8%, respectively from 2014]……One view of the decline in both large and small organisations reporting [in this survey] that they have insurance is that, having reviewed their policy details, these organisations have discovered that they are not as well covered as previously thought, or that insurers have taken steps to exclude cyber liability from general insurance policies.<br>In a nascent market, the terms and coverage of insurance policies vary tremendously; in turn, due to understandable caution, this may be preventing a larger uptake of policies than would otherwise be expected. This growth may be compounded by a lack of historical data, which makes it harder for insures to price cyber risk accurately.<br><br><u>Mobile Devices, Monitoring User Behaviour and Shaping Victim Status</u> |

| | | | | |
|---|---|---|---|---|
| | | | | Evidence from this survey demonstrates that organisations are beginning to manage the risks presented by mobile devices [smartphones and tablets], but we must not be complacent: One in five small organisations (18%) [of those surveyed] still have not taken any steps with the use of smartphones or tablets, even though the number of breaches through mobile devices [has] more than doubled. |
| Department for Culture, Media & Sport (2015a) | | Working with industry, we have started to transform business understanding and response, by getting cyber security out of the IT department and into the boardroom. | | <u>Cyber Essentials</u><br>If you adopt Cyber Essentials in your business, you will protect your business against the majority of threats on the internet.<br><br>I want to very clear about this. I'd like to see all businesses operating online adopt Cyber Essentials. [It] isn't just for the large prime firms. It also helps them to manage their third party risks, which is why we have made the scheme suitable for smaller businesses, including those which are part of larger supply chains. |
| Department for Culture, Media & Sport (2016) | | | | <u>Prevention</u><br>The majority, the vast majority of cyber attacks exploit basic weaknesses, whether it is in software, systems or people. All organisations need good basic cyber security. This can tackle the vast majority of attacks. |

| | | | | |
|---|---|---|---|---|
| | | | | Cyber Essentials and Shaping Victim Status<br>So, getting the simple processes right, that the Cyber Essentials scheme highlights, that is the easiest way to solve the cyber security challenge. It shows how firms can protect themselves against the most common online threats. It's equivalent to putting your takings in the safe and locking the door to the office. |
| Federation of Small Businesses (2015) | | | | Insurance and Shaping Victim Status<br>There are a number of products available to counter the growing cyber threat, and the industry believes that not enough businesses are taking advantage of these…….All small businesses should look into finding appropriate cover for their businesses.<br><br>Prevention and Shaping Victim Status<br>Too many firms ignore the threat of cybercrime. |
| GCHQ (2013) | | Educate users and maintain their awareness [as they all bear responsibility for cyber security]. | | |
| HM Treasury (2015) | | Government has a unique ability to aggregate and educate. | | |
| Home Office (2013) | | | | The Internet and online activities have now become central to the way people live their lives.<br><br>Shaping Victim Status |

| | | | | |
|---|---|---|---|---|
| | | | | Cyber-dependent and cyber-enabled crimes are not…just about technical skills, and rely heavily on the behaviour of the intended victim.<br>Use of public wi-fi is growing.<br>[Beyond the use of anti-virus software] Wider security practices are not universally undertaken.<br><br><u>Social Networking</u><br>YouGov (2012) reported that 52 per cent of UK citizens indicated that they would accept a friend request on Facebook from someone they did not know directly. |
| Home Office (2014) | [When businesses allow BYOD, they] should be aware of the potential security risks around potential malware infection and the compromise of corporate information.<br><br><u>Monitoring User Behaviour</u><br>Make sure that staff are made aware of which [remote working] solutions are approved for business use. | An educated workforce is the main line of defence against online threats in business. | Choose remote working options which offer an appropriate level of security for your business.<br><br>Consider the need for remote connectivity before opening up your network. If the main driver is access to files, then consider moving the storage of files onto a cloud service.<br><br>When storing personal data, especially on mobile devices...and removable media, encryption is highly recommended.<br><br>If your staff have to use public WiFi on any device, consider providing a secure VPN for them to browse | |

| | | | | |
|---|---|---|---|---|
| | | | through. Remember, not all public WiFi is encrypted – even if you are asked to enter a password.<br><br>Appoint a person in your organisation to be the point of contact (POC) responsible for ensuring that software is installed on new devices and they are configured correctly to run regular scans.<br><br><u>Managing User Privileges</u><br>Many pieces of software allow you to restrict staff from carrying out certain actions. It is best practice to restrict as many permissions as possible...so that staff only have access to the information and parts of the IT system they need. | |
| HoC Science and Technology Committee (2012) | While users should be expected to have protection, they should not be lulled into a false belief that it will solve all their problems. Technology needs to be understood in the wider context of safe online behaviour.<br><br>The covert nature of the threat means that the public and businesses can underestimate the risks. | Knowledge is the best defence against fear.<br><br>Television exposure is crucial to gain the widest possible exposure to the safety. | The public need clear identification of trusted information sources and relevant authorities and clear guidelines on how to help themselves stay free of infection.<br><br>We also recommend that the Government work with the industry partners announced in the Cyber Security Strategy to promote the equivalent of a 'Plain English' campaign to make the technology | For individual computer users, cyber crime is most likely to occur through casual infections and unfortunate happenstance. We have been told that the best defence against this kind of crime is more knowledgeable computers users, and that 80% of protection against cyber-attack is routine IT hygiene. |

| | | | | |
|---|---|---|---|---|
| | | | easier to understand and use. | |
| HoC Home Affairs Committee (2013) | It is of great concern that the majority of cyber crime could be prevented by better awareness by the user.<br><br>Witnesses from the police emphasised the importance of prevention through increasing people's awareness of the threats, and what they can do to protect themselves.<br><br>I hope the committee will consider the virtues of extending the notion of 'public health' to the cyber domain [Prof. Sommer]. | The Government and the private sector both have a strong incentive to educate users and maintain awareness of cybercrime.<br><br>We welcome teaching about online safety and security taking place in schools and initiatives such as Safer Internet Week.<br><br>I am not quite as enthusiastic about public education as some other people, because…computers and mobile phones and social networking sites tend to ship with unsafe defaults because it is better for selling advertising [Prof. Anderson].<br><br>There is a lot to be said for helping people to help themselves [Prof. Sommer].<br><br>I notice that out of a total of £650 million for the overall [National Cyber Security] programme, Get Safe Online has received just under £400,000 (0.06% of the total budget) [Prof. Sommer].<br><br><u>Social Engineering</u><br>One of the big concerns in e-crime is the extent to which social engineering methods are deployed, and education is the principal means by | We surely need much more frequent Government-sponsored official advice. Inevitably, commercially sponsored advice pushes the public towards the specific products and services of the sponsors [Prof. Sommer]. | Some of the research we have been involved in has been looking very specifically at the bleed between domestic lives and work lives. If people are engaged in these kinds of technologies in their domestic lives, could that be used to introduce vulnerability into the enterprise through more enhanced targeting? In truth, probably yes, we are in a situation where that could be the case [Prof. Creese].<br><br><u>Prevention</u><br>No matter how good your information security information is, even companies like Google – real-world experts in doing it – are not going to be able to defend against every attack [Prof. Brown]. |

| | | | | |
|---|---|---|---|---|
| | | which it can be spotted and thwarted [Prof. Sommer]. | | |
| HoL Science and Technology Committee (2007) | | <u>Prevention</u><br>The key [is] that products should be developed in such a way as to educate consumers about risks and to provide them with the tools to manage these risks. | | |
| Symantec (2015) | | | | <u>Shaping Victim Status</u><br>Last year, 60 percent of all targeted attacks struck small and medium-sized organisations. These organisations often have fewer resources to invest in security, and many are still not adopting basic best practices…This puts not only the businesses, but also their business partners, at higher risk. |

# Appendix H

**Listing of the thematic framework used in the analysis of the data collected during the Case Studies.**

Matrices

**1 Policy**

1.1 Engagement with policy

1.2 Disengagement from policy

1.3 Practice without policy

**2 Practice**

2.1 Engagement with policy

2.2 Disengagement from policy

2.3 Practice without policy

**3 Contextual influences on behaviour**

3.1 Financial

3.2 Personal

3.3 Professional

3.4 Technological

Headings (for more specific categorisation within those Matrices)

'An IT Dept Issue'
Blame
'Common sense'
Cyber insurance
Cyber security
Cyber Streetwise campaign
Cyber Essentials scheme
Formal guidance
Informal guidance
Managing user privileges
Remote working
Responsibilisation
Risk
Social engineering
Social media
Training
Work/personal divide
Work pressure

# Appendix I

**The data from both stages of the Case Studies (Diary Study and Interviewing) set within the thematic framework.**

## 1. Framework matrix for the 'Policy' theme

| 1.1 Dissemination of policy | 1.2 Awareness of policy | 1.3 Absence of policy |
|---|---|---|
| <u>General</u><br>The trouble is, you get the impression that it's an ever-moving field of crime. And just having a policy in place might protect us in a certain way if we were sued by somebody else, but it might not actually work…Because that's what policies are for, generally. In employment, you have your staff handbook. It's helpful to the staff, but mainly they (the policies) are there to protect you (as the employer). So, I think there is a danger of having a policy and it just remaining in an office manual. And probably being nagged on a weekly or monthly basis by the IT Manager is better in many ways [P25/B/Int].<br><br>If you just send someone a policy, and say 'stick this in your copy of this the office manual,' they will just ignore it…In fact, quite often they would probably just delete it, without doing anything….I do it myself [P25/B/Int].<br><br>I have just disseminated a new policy to my department. I don't know whether it has been disseminated to the rest of the staff. We do act in little, rather ad hoc groups within the firm, as I'm sure most businesses do [P25/B/Int].<br><br>They [the firm] do have certain things in place [policies concerning cyber security]. But I'm not sure that safeguards are necessarily known about *throughout* the business; they are not really communicated that well [P24/B/Int]. | <u>Cyber security</u><br>The IT Manager is a man on a mission with it (cyber security). And we have Directors who are apoplectic with fear. So, there is much awareness of it [P16/B/Int].<br><br><u>Cyber Streetwise campaign</u><br>**Are you aware of the government's *Cyber Streetwise* campaign?**<br><br>No (25 of the Participants).<br><br>I've heard of it, but I don't know what it is. I think it might have been on the telly, actually. I think there was an advert about it (P7/C/Int).<br><br>Well, I'm only aware of it because I've seen a couple of posters about it; billboard-type posters. And I can't remember which one I saw, but I scoffed at it….I think I had just seen it after the government had had some huge data leak of some sort or another, and I thought it was a bit rich [for them] to be telling everybody else [what to do] (P1/A/Int).<br><br>I certainly am, I've visited the website. I've also even seen an advert for it on a poster at the bus stop. But I should also point out that I only discovered the website because I was searching for cyber security information online – I was looking for some free, educational posters – and I found [a link to] it on a government website (P18 (the IT Manager)/B/Int).<br><br><u>Cyber Essentials scheme</u><br>**Are you aware of the government's *Cyber Essentials* scheme?** | <u>General</u><br>We are under quite heavy financial pressure the whole of the time. So, writing a cyber security policy doesn't do well in the prioritisation wars with phoning a customer or delivering the service. So, that's why it hasn't happened. It's not that I don't think it's important. But, on the scale of things, it's one of these things that is a job that's constantly getting postponed [P1/A/Int].<br><br>We should have tighter procedures and practices than we have, and a little bit of inconvenience is trivial compared to the risk and consequences of being hacked [P1/A/Int].<br><br>I think – particularly with the unexpected turnover in certain roles within the company – that it would be prudent to have a measure of policy [P2/A/Int].<br><br>Yes, the more I think about it, the more I ask: 'Why *don't* we have a cyber security policy?' [P6/C/Int].<br><br>I don't think there's a specific policy in place at the moment, in terms of staff following protocol. But we are all aware of it (cyber security) now [P20/B/Int].<br><br><u>'Common sense'</u><br>I think it just comes down to common sense a lot of the time, rather than a rule saying 'you must keep an eye out for this.' Because attacks and viruses could come in all shapes and forms. And you could have a list as long as your arm of things that you could, potentially, keep |

| | | |
|---|---|---|
| Formal guidance<br>**Do you think that your work colleagues would welcome more formal guidance on cyber security?**<br><br>I would hope so. But the plan is to give it to them, anyway [P1/A/Int].<br><br>Yeah, a bit of, say, awareness off things [P2/A/Int].<br><br>I think they would. Frankly, as the CEO, I don't care whether they would or not; they're going to get it [P4/C/Int].<br><br>My guess would be yes. I think that quite a lot of my colleagues are not particularly IT-savvy. Some are, but plenty aren't. There's a danger of kind of overloading people with guidance, that ends up being ignored because it's just too much. But yes, I guess people would, probably [P5/C/Int].<br><br>Yes. There is a lack of knowledge. As I was saying, we don't know how a network works, and if everything has to be protected, or not. And particularly with some people who perhaps aren't as computer-literate as others. We had quite a long – in fact, arduous – training session on *Twitter*, so that's the kind of level [P6/C/Int].<br><br>I think yes, probably, because of the incident that we had. And the fact that we get some weird emails [P7/C/Int].<br><br>Yes, I think they would [P8/C/Int].<br><br>Yes, probably [P9/C/Int].<br><br>Yes [P10/C/Int].<br><br>As long as it's understandable and usable. It's not about whether we all welcome it or not [P11/C/Int].<br><br>I think possibly. We are seeing a massive increase in | No [27 of the Participants].<br><br>Yes, I am; the accreditation scheme [P18 (the IT Manager)/B/Int].<br><br>Remote working<br>**Does the business that you work for have a remote working policy?**<br><br>**Business A** (has no policy)<br>No [P1/A/DS].<br><br>Not a formal policy [P2/A/DS].<br><br>I don't know [P3/A/DS].<br><br>**Business B** (has a policy)<br>Yes, it does [P20 and P26/B/DS].<br><br>Yes, it does. We don't just let anybody do it (remote working). So, they do have to get permission, yes [P15/B/DS and Int].<br><br>Yes, although I don't know what it is [P12/B/DS].<br><br>As far as I'm aware, it does not have one. And that alarmed me, actually, because I tend to write our policies. But it is difficult to know what to put in it, because we all work differently [P25/B/Int].<br><br>I'm unsure about this. We have policies about everything though, so I'd be surprised if we didn't! [P19/B/DS].<br><br>I don't know [P13, P14, P16, P17, P18, P21, P22, P23, P24, P27, P28 and P29/B/DS].<br><br>**Business C** (has a policy)<br>Yes [P4, P7 and P8/C/DS].<br><br>Yes, I think so [P5 and P9/C/DS].<br><br>Yes, but to my knowledge it is only about health and safety when working from home or personal security when meeting new people outside of the office, not about remote working from a cyber security point of view [P6/C/DS]. | an eye out for. It's good to be mindful of them, if they're particularly obvious ones that are really easy to spot. The less obvious ones?<br>I think you can only really confront them when they happen, regrettably. [P2/A/Int].<br><br>Responsibilisation and Blame<br>We don't have a policy that would say there would be disciplinary action in those circumstances (a phishing email attack), unless there was some malicious action, or if it was clearly negligent, I guess there could be. But if it was just a clever ruse, I don't think that you could hold an employee responsible for opening an email (or an attachment to it) purportedly sent to them by a colleague [P25/B/Int].<br><br>Risk<br>Yes, there is no (remote working) policy….My son's laptop (that I sometimes use at home for work purposes) is probably especially risky because he's on *TOR* and *4chan* and all kinds of things like that [P1/A/Int]. |

| | | |
|---|---|---|
| (Solicitors) firms being attacked. And everyone is busy, but I think we are all very aware of the risk of being attacked [P12/B/Int].<br><br>Yes, definitely. And, as a firm, I think we need it, definitely [P13/B/Int].<br><br>I think it's useful to be reminded a bit, regularly. And to be updated about what's happening to other businesses, with what's out there. Just keep everyone up to date. And not too formally; just to approach the IT Manager if you have got something on your mind, or something that you're concerned about [P14/B/Int].<br><br>Probably. I mean, we do have a policy – I don't think it's particularly formal – but we are looking into it at the moment. And this study has further concentrated our minds on it. Yes, because I think that everybody appreciates having a set of rules which they know, if they are broken, then we are in trouble [P15/B/Int].<br><br>Broadly speaking, yes. But I imagine there are a few people here who would rather just have their head in the sand, and I don't think they'd welcome formal guidance on anything, let alone cyber security. But I think that the majority would welcome it, and do it. But it's a difficult thing to do, I appreciate. And you would get some people who would object to it, and to any sort of formal training [P16/B/Int].<br><br>Yes, of course they would [PP17/B/Int].<br><br>I think that they would like to gain more knowledge on it, without having to put a lot of effort into doing so [P18 (the IT Manager)/B/Int]. | Not as such. It would be useful to have some pointers as to what to include if we do put one in place [P10/C/DS].<br><br>I'm not sure [P11/C/DS].<br><br><u>Risk</u><br>**Does the business that you work for have a formal policy/procedure for reporting risks and incidents which (are thought to) have either threatened or breached the company's cyber security?**<br><br>**Business A** (has no policy)<br>No [P1/A/DS].<br><br>No procedure, but these events become self-evident [P2/A/DS].<br><br>I don't think so [P3/A/DS].<br><br>**Business B** (has no policy)<br>Not a formal procedure, although if I receive anything suspicious I forward it onto our IT Manager [P12/B/DS].<br><br>There is a policy for reporting risks or concerns for different areas, such as money laundering. But I do not believe that there is a specific policy on cyber security [P13/B/DS].<br><br>I'm not sure whether there is a formal policy. You just need to let the IT Manager know [P14/B/DS].<br><br>Yes. We are always receiving emails regarding various frauds or scams or spams. The IT Manager tells us what to look out for [P15/B/DS].<br><br>I am unsure about whether there is a formal policy. I would assume that it is common practice to report it to our IT Manager, and this is what I do [P16/B/DS].<br><br>I don't know [P17/B/DS].<br><br>No [P18/B/DS].<br><br>I'm not sure [P19/B/DS]. | |

| | | |
|---|---|---|
| I think they probably would, because I think that there is a bit of a fear of the unknown. And I think that if everybody knows exactly what to look out for – although I know that's difficult – and exactly what to do if they did see something [P19/B/Int].<br><br>Yes. The more the better, basically. I think it just needs to be drilled into everybody that it's a serious threat. And people need to always have it in the back of their minds, throughout the working day. And not think: 'Oh well, I'm not going to be targeted.' Because they might be. So yes, I think everybody should have as much guidance as they can [P20/B/Int].<br><br>'Welcome,' I don't know. But obviously, working in this industry we do need to have all these things. But I don't know whether people are overly enthusiastic about attending all these things. So, I don't know if 'welcome' is the word I would use….But it needs to be done, really [P21/B/Int].<br><br>I guess so. Policy like that would always help. But I think that everyone would know to report it to their Line Manager, who would, in turn, report it to the necessary person. Erm…, yeah, I suppose there would be no harm in it. Knowing exactly what to do, and what to look out for. And what to do in the event of something happening [P22/B/Int].<br><br>Yes, I think it's really important. I think that, even though we receive emails (from the IT Manager), when people are having a busy day at work it is easy to open an email, read it once, think 'I've read that, that's done,' and then just delete it, or skim read it and not take everything in properly [P23/B/Int].<br><br>I guess it's good to have that background information. But, | I'm not sure. I don't think so [P20/B/DS].<br><br>I'm not sure that there is any particular policy, but I would usually refer to the IT Manager [P21/B/DS].<br><br>I'm not sure, although I would imagine any issues would be reported to our IT Manager [P22/B/DS].<br><br>I do not know [P23/B/DS].<br><br>I'm not sure [P24/B/DS].<br><br>All the IT issues are reported to the IT Manager [P25/B/DS].<br><br>Yes [P26/B/DS].<br><br>I don't know [P27/B/DS].<br><br>Yes [P28/B/DS].<br><br>I am sure that there is something in our office manual about this, but I don't know specifically. We have, however, been asked to refer any IT-related issues to our IT Manager for him to deal with [P29/B/DS].<br><br>**Business C** (has no policy)<br>No formal policy, but I am fairly sure that all of us would report such things to the Office Manager, who is the main link with our IT Support provider [P4/C/DS].<br><br>I think it does [P5/C/DS].<br><br>I don't know. It may come under ISO 9001, but I wouldn't know what to do if it happened to me [P6/C/DS].<br><br>The formal policy or procedure would be to let the Office Manager know by email or by telephone [P7/C/DS].<br><br>Yes. An email came in and we were suspicious of it, and I was advised to delete it [P8/C/DS].<br><br>As a charity, I believe we have to report anything to the Charity Commission [P9/C/DS]. | |

| | | |
|---|---|---|
| at the same time, I know from experience that when the IT Manager sends round emails about stuff like that, they generally just don't get read. And I think that maybe once or twice a day he will send them, and I think that a lot of people choose not to read them [P24/B/Int].<br><br>Probably, being nagged on a weekly or monthly basis by the IT Manager is better in many ways (than having more formal policy) [P25/B/Int].<br><br>Yes, I think so. I think that forewarned is forearmed, isn't it? So, I don't think you can ever have too much knowledge, or information being passed on [P26/B/Int].<br><br>Yes [P27/BB/Int].<br><br>I can't see that it would hurt. I think it would just be seen as another round of training, to do x, y and z. These things are an inevitable part of modern day office life [P28/B/Int].<br><br>Potentially. At the moment, we are being given a lot of new procedures to follow. But if there are ways that we can further safeguard ourselves – which we are not already doing – then people would welcome some further information [P29/B/Int].<br><br>**For you personally, what would be the best way to deliver that further guidance on cyber security?**<br><br>I think that people like group sessions. I probably would [P1/A/Int].<br><br>I think intensive cyber security training would – not necessarily not be relevant – but would not necessarily be in my thinking. Everyone works differently. Everyone's mind works differently. Whilst I'm technologically able, I'm not a techie, if that makes sense. | As part of ISO 9001, we have a non-conformance reporting procedure, and this is what we would, and have, used for reporting incidences of threats or breaches of cyber security (e.g. with the Crypto Wall virus last year). These non-conformance reports are reviewed by senior management [P10/C/DS].<br><br>I'm not sure [P11/C/DS].<br><br><u>Social media</u><br>**Does the business have a policy on employees' use of social media?**<br><br>**Business A** (has a policy)<br>Yes, it does [P1 and P2/A/DS].<br><br>I don't think it does, but I'm not 100% sure [P3/A/DS].<br><br>**Business B** (has a policy)<br>Yes, it does [P12, P13, P14, P15, P16, P17, P18, P19, P21, P25, P26, P28 and P29/B/DS].<br><br>I believe that social media use at work is not particularly wanted, and should be kept to a minimum [P24/B/DS].<br><br>I know that we have a policy, although I'm not entirely clear on it [P27/B/DS].<br><br>There is a policy, but I'm not sure what it is [P20/B/DS].<br><br>I don't know [P22 and P23/B/DS].<br><br>**Business C** (has a policy)<br>Yes, it does [P4, P5 and P10/C/DS].<br><br>I think so, [but] I am not sure where to find it [P9/C/DS].<br><br>I'm not aware of one [P8/C/DS].<br><br>I don't know [P6, P7 and P11/C/DS].<br><br><u>Cyber insurance</u> | |

| | | |
|---|---|---|
| And I think there's a subtle difference. And, as a result, I think a lighter level of cyber security awareness, maybe, would be useful, just to keep an eye out for tricks and whatever, beyond the sort of stuff that you pick up as you go along [P2/A/Int].<br><br>One workshop which establishes some key principles; things that I would then be able to follow on a regular basis….And I think that putting it into the appraisal system would be a very good idea [P4/C/int].<br><br>For me personally, as long as it [the email message] was fairly short [and was saying]: 'Here's a new policy, here's what you need to do, here's the detail, go and read it.' That would work for me [P5/C/Int].<br><br>I think via a workshop. I've done a few online courses, and I've never really come away thinking: 'I've got that.' In fact, we've recently had some workshops and I actually really enjoyed them for the opportunity to get together with the other members of our team, and to discuss problems which were are all facing [P6/C/Int].<br><br>It would have to be something that fits into your day, for which you're not having to do extra work. I don't know whether you could put things around the office; you know, like reminders. Up on the screen would be a really good idea. Maybe when you log on in the morning. Or it just pops up now and again. Just to prompt you. As a reminder [P7/C/Int].<br><br>For me personally, ideally it would be one-to-one guidance. Or a group guidance with somebody perhaps doing a talk, or something. I think I probably learn more if I have that. Whereas, if an email just comes in, I don't always have | **Is the business insured against cyber security risks?**<br><br>**Business A** (not insured)<br>We aren't, but I'm thinking that we should be [P1/A/DS].<br><br>I'm not sure [P3/A/DS].<br><br>I don't know [P2/A/DS].<br><br>**Business B** (not insured)<br>No, it isn't [P20 and P21/B/DS].<br><br>I'm not sure [P14, P19, P22, P24, P26, P27/B/DS].<br><br>I don't know [P12, P13, P17, P25, P28 and P29/B/DS].<br><br>I believe so, but I am not 100% sure [P23/B/DS].<br><br>Yes, I think it is [P15/B/DS].<br><br>Yes, it is [P16 and P18 /B/DS].<br><br>**Business C** (not insured)<br>I'm pretty sure that we're not [P4/BC/DS]. Even though they didn't have to pay out for the incident that we fell victim to, we were still required to inform our insurers about what had happened, which is a bit of an uneven relationship! But we should probably explore changing the insurance [P4/C/Int].<br><br>I think that I ought to know this, but I don't [P10/C/DS].<br><br>I don't know [P5, P6, P7, P8, P9 and P11/C/DS]. | |

| | | |
|---|---|---|
| time to spend and take it in. So, for me, probably that would be my preferred way of learning [P8/C/Int].<br><br>A training day, because you can write policy and send it to us by email, and we can click it and skim read it in ten seconds, and then just get back to our work. But if you pull people away from their desks, they *are* going to listen, they *are* going to understand. They've then got the time to take it in, digest it. And then they know what to do. Whereas, just reading something that's been sent is…….well, it's good that it's been sent – so, definitely back-up notes after the training – but I like to be told *in person*……So, in an ideal world, one training day, and then a refresher every six months or a year. And with a back-up document, with a drawn out policy that you could refer to [P9/C/Int].<br><br>Maybe a training session, I think. Or perhaps it could be part of a staff meeting [P10/C/Int].<br><br>Workshops. Workshops where you can see, you know, how easy it can be to be got, and how much damage it could cause [P11/C/Int].<br><br>Probably in meetings, because if you click on an email you might have a scan through. Whereas, if we were sat down in small groups, I think that would be the best way, because you have to pay attention and listen to it; rather than just sending an email, which 90% of the time you would just quickly scroll through. So, probably small group meetings would work, with updates and visual examples. That would work….And I think that real-life examples always help as well [P12/B/Int]. | | |

| | | |
|---|---|---|
| Every quarter there is a meeting which everybody attends, in the Conference Room. And actually, it's quite a good way, because everyone is there, and it's not too long a meeting – so people don't get bored – and it also starts the conversation, and they are allowed to ask things, or they will come and see me after the meeting [P13/B/Int].<br><br>Well, I think that emails without paragraphs and paragraphs of formal stuff. And also, when it's a story about someone else – like one recently of a Solicitor who was tricked into transferring over clients' money – it makes you realise how real it is, and how current it is….(and) that it could happen to you, and here's an example of it. I think that you probably do need to be regularly reminded of the risks and dangers [P14/B/Int].<br><br>I would prefer it in an email. That's what we tend to do with all our policies. When we've written a new section in the office manual, everybody gets emailed on it. And the email either says 'go to this section to print it off,' or it says 'here it is attached for you.' I mean, I personally need a bit of paper. So, I would appreciate an email, and then I can print it off [P15/B/Int].<br><br>I personally think that we should have training sessions. After attending this course last week, it's terrifying. And it needs to come down to every single member of the firm. Everybody needs to know what these criminals are doing. Everybody needs to know what to look out for. And I don't think that everybody's aware, necessarily [P19/B/Int].<br><br>That's a tricky one. I don't that there should be cyber security overload. You know, sitting there for half a day, watching videos or having seminars. Because it's just not going to | | |

| | | |
|---|---|---|
| go in, is it? You'd probably get bored after about half an hour. Maybe just workshops. And reporting of real-life examples. Just in small doses, you know. Just maybe weekly reminders, to try and make sure that people don't forget, and that people are on the ball. I don't think that the guidance should just come via email, either. I think a lot of people don't read emails, so I don't necessarily think that the IT Manager sending round emails all the time is that effective; I don't think people will read them [P20/B/Int].<br><br>It's better to have presentations and stuff, rather than just written formal policies. How much people read those things, I don't really know. Even where some of the emails are labelled 'All Staff' or 'Urgent' or 'Must Read' or 'Critical,' I think most people would only skim-read it, at best, anyway. And the thing is that it's one of those things where it's quite useful to give examples which are quite visual. You know, you can give examples of fake emails, etc. So, I think it's probably one of those things where it's better to discuss it *orally* than to have just some written procedure [P21/B/Int].<br><br>I suppose that I'm more like a visual person. I'd like some kind of presentation, or something like that, with actual examples of what an email that is designed to trick you might look like [P22/B/Int].<br><br>I think that, even if it was just something – whether it was a presentation, or having discussions with separate groups or departments, or whatever – to say: 'This is what you need to look out for. This is where it's likely to be.' And useful things like…, you know when go for a driving awareness course – I haven't been myself, but I know people who have! – and the | | |

| | | |
|---|---|---|
| instructors say things like: 'It's most likely to happen at this time of day, in this kind of environment, and in this kind of weather.' Even things like that…, if (on the subject of cyber security) someone were to warn you that things are most likely to happen on a Friday afternoon when people are (mentally) more switched off [P23/B/Int].<br><br>I think probably in a meeting, face-to-face [P24/B/Int].<br><br>I think that we would probably have a staff meeting [P25/B/Int].<br><br>I think maybe a workshop. Because I always think it's better when you are in a group, listening to someone who is giving a talk. And you are more likely to take it in and remember everything, and you can make notes. Whereas, if you get it in an email, you are likely to think 'have I got time to read this?' And you keep putting it off, and putting it off. It's just more likely to stick if it's given out in a workshop. A bit like we are now; just tossing ideas around, and brainstorming, I suppose [P26/B/Int].<br><br>If we had like a little meeting, or something like that. Rather than an email….Sometimes you'll get emails, and you think 'I'll just read it later,' but then you don't read it….So, face-to-face meetings to give out formal guidance would be good [P27/B/Int].<br><br>I think that, given the size of this firm, perhaps two or three group training sessions, where perhaps you have an opportunity as well to discuss best practice, discuss individual case studies, and actually as an interactive session. If it was simply, say, training on the PC, and something that we were told that we had to do, perhaps the message wouldn't be quite so forceful, (and) | | |

| | | |
|---|---|---|
| integrated? It would just give us a clear space of time to understand the issues, understand what we need to do and, as I say, raise any concerns [P28/B/Int].<br><br>Well, I have found this very helpful. So, to have a session maybe, where someone came in to explain what different things meant, and where and how to be careful, would be good. And also including a Q&A session….(And) I think the other thing is that, at the moment, I find the whole thing quite daunting. And you can become quite overwhelmed by it, and quite scared by it. So, if somebody actually sat down and said 'yes, you've got to be careful, but this is actually what's going on, and this is what you have to protect,' you know [P29/B/Int].<br><br><u>Training</u><br>**Have you had any training on cyber security whilst working for this business?**<br><br>**Business A**<br>We had a consultant come in and do an audit, and he fed back some areas of weakness. As a result, one of the employees (X) went on a training course, but he's left now. [P1/A/DS].<br><br>The only training that's taken place is that one-day course that I sent X on. That's it [P1/A/Int].<br><br>Nothing. Zilch [P2/A/Int].<br><br>**Business B**<br>Verbal and written communications from our IT Manager [P12, P14, P15, P16, P25, P26, P27, P28 and P29/B/DS].<br><br>We have emails sent to all staff, and occasional meetings where the subject is brought up [P19/B/DS].<br><br>Only emails, when there is a threat…, and it has been briefly | | |

| | | |
|---|---|---|
| touched on at quarterly staff meetings [P13/B/DS].<br><br>Not from the business, but from external partners (verbal and written) [P18 (The IT Manager)/BB/DS].<br><br>None that I can remember [P23 and P24/B/DS].<br><br>None [P17, P20, P21 and P22/B/DS].<br><br>**Business C**<br>We have received guidance from our IT support provider. The format has varied: email, telephone, face to face, and web-based [P4/C/DS].<br><br>Written (some elements in our staff handbook), verbal and visual. During Induction, and then occasionally in staff meetings [P5/C/DS].<br><br>Yes, in written and verbal form, provided by someone in the business (but they acquired it from another organisation) [P8/C/DS].<br><br>Yes, but I can't remember it [P11/C/DS].<br><br>We were given Induction training on how to use spam filters and safe password use. Our IT Support provider gives ad hoc advice, which is conveyed to staff by email. It would be useful to have some further pointers, to ensure that we are giving staff adequate information and ensuring that we are 'cyber safe' [P10/C/DS].<br><br>I was told by the Office Manager that if the web browser prompt 'Do you want Chrome to save this password?' comes up, not to save it. That is the only training on cyber security training I have had [P6/C/DS].<br><br>I don't think so, but I must admit that I do not spend much time reading policies. When I started the job, I spent my time reading about things I will be doing in my job, so may | | |

| | | |
|---|---|---|
| have glazed over something about cyber security, but would not be sure as it is not something that would interest me. If we did, it would have been in written form [P7/C/DS].<br><br>None [P9/C/DS]. | | |

## 2. Framework matrix for the 'Practice' theme

| 2.1 Engagement with policy | 1.2 Disengagement from policy | 1.3 Practice without policy |
|---|---|---|
| <u>General</u><br>I mean, everywhere has got formal policies for everything. So, a formal policy is one thing, but that's not necessarily what makes the difference. It is the practice [P16/B/Int].<br><br>I think that, generally, the mindset is that if you've got a set of rules that you have to follow, then you just follow them [P15/B/Int].<br><br>I think it's important to have those procedures and policies in place. At the end of the day, everyone wants to follow the procedures….I think it can be done, and I think that, as soon as you have adjusted to it, it doesn't actually affect your time balance, because you are already used to it; it's just that easing into it stage…And people need to know that it is achievable (the policy); that they actually can do it, and incorporate it into their day. Whereas, if it [policy] is thrown in or launched too quickly, then it's immediately going to cause friction [P23/B/Int].<br><br>I don't want the responsibility of anything going wrong because of me, so I will naturally just do that. I just think that it's common sense, | <u>General</u><br>I have to regularly remind people – and not just internally, but the other organisations that we support – that if you've got a policy on something, it's there for a reason, and actually the worst thing you can do if you've got a policy is to ignore it [P4/C/Int].<br><br>It's sort of assumed that perhaps the IT guys deal with that (cyber security) [P6/C/Int].<br><br>It's quite hard sometimes to get everybody to do stuff. You know, you pass on the information to staff, but whether they are doing it in reality……it's hard. You feel like you need to assume that staff can follow instructions. But whether they are actually doing it in practice….Maybe there needs to be some sort of auditing every so often of whether they are doing it [P10/C/Int].<br><br>Yes, there might be (a danger of reminder fatigue). Particularly in my department, because I do Conveyancing. And obviously, we are the most likely target. We *do* talk about it *all* the time [P15/B/Int].<br><br>Probably, yes (there is a risk that people either don't read those policy emails, or just skim read | <u>General</u><br>Because I'm quite new here, I sort of like to ask, just in case they (my work colleagues) know something that I don't know [P24/B/Int].<br><br><u>'Common sense'</u><br>I think it just comes down to common sense a lot of the time, rather than a rule saying 'you must keep an eye out for this,' because attacks and viruses could come in all shapes and forms. And you could have a list as long as your arm of things that you could, potentially, keep an eye out for…It's good to be mindful of them, if they're particularly obvious ones that are really easy to spot. The less obvious ones…I think you can only really confront them when they happen, regrettably. [P2/A/Int].<br><br><u>Risk</u><br>**Given that there isn't a formal policy/procedure on reporting risks and incidents, if you became aware of a threat to the business's cyber security, what would you do?**<br><br>**Business A**<br>Well, if I think there's a threat, I'd notify P1 (the owner of the Business), because he has ultimate control over everything. So, I'd tell him that I think it's a |

| | | |
|---|---|---|
| that if the IT Manager isn't there, I would need to find the policy and I would check the Intranet. And if it's not there, then I would need to go to HR. And you just follow a stream. It's not anything that I've been told to do, or I think is right. It's just what I believe is common sense [P26/B/Int].<br><br><u>Cyber security</u><br>**Do you ever feel that your ability to do your job is hindered by cyber security considerations, rules or practices?**<br><br>No [P1/A/DS and P4, P5, P6, P9, P10 and P11/C/DS and P12, P14, P16, P17, P18, P19, P20, P21, P22, P23, P24, P25, P27 and P28/B/DS].<br><br>I don't feel that it is hindered, although it is something we have to be incredibly aware of and<br>concerned about, especially when dealing with clients' bank accounts and money [P12/B/DS].<br><br>Not hindered, but I do feel the need to be alert to cyber security, and this is something which is increasing daily [P26/B/DS].<br><br>Not really, but it's always something to consider [P3/A/DS].<br><br>Rarely [P2/A/DS].<br><br>Sometimes. You have to be so careful. It has added extra steps to the process, because you need to check third parties all the time [P15/B/DS].<br><br>We have to do a lot of checks, and this is time-consuming, and therefore prevents us doing something else; so yes, in a way [P29/B/DS].<br><br>Yes, given all the concerns over bank details in emails now, and fraudsters setting up bogus law firms, and | them). But, I mean, when you've got about 50 people, it's difficult to know how else to do it. I mean, we have in the past sent round a memo, and everybody signs it off once they've seen it. But there's also a tendency for people just to sign it and hand it on to the next person, anyway. So, it is a bit difficult [P15/B/Int].<br><br>I imagine there are a few people who would rather just have their head in the sand, and I don't think they'd welcome formal guidance on anything, let alone cyber security [P16/B/Int].<br><br>I suppose that it's one of those things where it is fundamentally a culture change. So, you wouldn't want to be hitting it too hard all the time, because people will become alienated from the principle, and they will just begrudge it. And that's not helpful. Because the problem that we have at the moment is that, you know, we are having a *lot* of chats about cyber security, there is a growing awareness, and people are scared of it. So, the more you hammer it, the more scared of it they become, and that doesn't necessarily help. So, I think sometimes you can overplay it. Not overstate its value or importance, but just in terms of the buy in that you get from the staff; if you hit it too hard, too often [P16/B/Int].<br><br>To some extent, he (the IT Manager) is doing a good cop, bad cop all by himself….And sometimes he's trying to make an impact – because he doesn't feel that people are engaging with it – and sometimes what he is doing is pushing people further away. And I have said that to him….It's difficult, because he wants to get a response from people. And there's a little bit of the sports mindset of: 'I want to make them angry, so that they perform properly.' But that doesn't work for everyone [P16/B/Int]. | real hazard. If he doesn't deem it to be a hazard, then I would usually bow to his superior knowledge in terms of technical things. In which case, you know, I would go with whatever he says [P2/A/Int].<br><br>Well, what I would expect P2 to do is to come and tell me about it as soon as he discovered it. Erm, I think in his case the question might be whether he would recognise a threat [P1/A/Int].<br><br>**Business B**<br>I would report it to the IT Manager….Just because he is the IT guy. And I figure that, out of everyone in the firm, he's most likely to know what something is. The Directors aren't very tech-savvy themselves. If they were, I might report it to them first, instead….But there's a general acceptance that if someone receives something dodgy, they just forward it to the IT Manager and let him deal with it [P12/B/Int].<br><br>I would speak to the IT Manager straightaway…because he's the IT guy. Everybody goes to him…And if he wasn't here, then he leaves us with lists of numbers for all our IT people, so I would ring them and say I'm a bit concerned [P13/B/Int].<br><br>Well, I put emails into junk email if I don't think they are right. Or, if I'm not sure whether it should be opened or not, I'd send it to Participant 18 (the IT Manager) [P14/B/Int].<br><br>Well, as far as I'm concerned there is (a policy), because it's in our office manual, and you basically have to report everything that's even vaguely suspicious to the IT Manager. Even if you just think it *might* be suspicious, you report it to him, and he checks it before you actually look at it – an email, or whatever… That is what we are supposed to do, because we are supposed to be reporting these risks to him, so he can then tell |

| | | |
|---|---|---|
| hacking emails in genuine conveyancing transactions, many more checks have to be done, incurring more time [P13/B/DS].<br><br><u>Managing user privileges</u><br>And then there's the own equipment question, which is: Is somebody likely to sign up to me being able to remotely wipe their phone if they lose it, just because it's got access to the company's documents on it? Ideally, I would like to say: 'This is your company mobile phone, do not use your personal mobile phone at all for anything to do with this company' [P1/A/Int].<br><br><u>Responsibilisation</u><br>I would say that in all organisations like this, I (as the owner) am ultimately responsible for everything. But everybody has got a responsibility for following what the policy says [P1/A/Int].<br><br>And a lot of these kids coming out of college, they know enough about computers and about how the Internet works, and about how networks work, to realistically expect them to be able to learn about this stuff and take responsibility [P1/A/Int].<br><br>And it might also be wise to put something in their contract of employment; some specific terms relating to cyber security and their responsibilities; it makes it explicit [P1/A/Int].<br><br><u>Risk</u><br>We have this ISO 9001, under which we are supposed to report things that have gone wrong, or incidences and that sort of thing. And I only generally think to report things to that at about 3am, two days later. Normally, I | Emails going out are great, but people just don't read them, and put them into a folder, or delete them [P17/B/Int].<br><br>I don't think that the guidance should just come via email, either. I think a lot of people don't read emails, so I don't necessarily think that the IT Manager sending round emails all the time is that effective; I don't think people will read them [P20/B/Int].<br><br>I know from experience that when the IT Manager sends round emails about stuff like that, they generally just don't get read. And I think that maybe once or twice a day he will send them, and I think that a lot of people choose not to read them [P24/B/Int].<br><br>I think that it's very easy just to skim past an email, delete it, and then tell someone that you've read it. I know that within his emails the IT Manager says: 'Please do read this, and don't ignore it.' But I'm sure that a lot of people do just still ignore them. I know that in the past he (the IT Manager) has spoken in quarterly meetings about these types of things, and just gone over the main issues. But, I almost think that people just get a little bit bored of hearing about the same thing, like all the time. Then people start to switch off a little bit, and it's like you're constantly being given all this information……. As well, a lot of his emails are in IT language, and stuff like that, and a person like me doesn't really understand that, anyway, if I was to read it. I just think that it goes over your head a little bit [P24/B/Int].<br><br><u>'An IT Dept issue'</u><br>I assume that when I am at work that cyber security is already being dealt with by various different softwares that are installed [P24/B/DS]. | everybody else to look out for them [P15/B/Int].<br><br>I would telephone the IT Manager…Because he's told us (to do that). We have quarterly meetings, and at the last one he talked about cyber security, and he was repeatedly saying: "If anything comes up, call me." If he wasn't here, other than calling him repeatedly on his mobile phone, to be honest with you, I wouldn't know what to do. I'd probably make most people aware of it. But there's not anyone else that I would think: 'I need to tell this person, and they will deal with it.' I don't know what the fallback plan is, at the moment, to be honest [P16/B/Int].<br><br>Formal policy is different from using your common sense. And we've got a computer guy on site, and there's absolutely no problems with any answers; he deals with it immediately. And I know that he's got the facilities to check these emails and attachments, and that kind of thing. But an actual formal policy where it's written down…? Maybe in the Office Manual? I just don't know [P17/B/Int].<br><br>I would go straight to the IT Manager, because he's in the office next door to mine. I'd say to him: "This looks weird. Help." Anything that looks out of the ordinary. Anything that I think isn't normal. Anything that looks a bit strange. Anything that I'm not expecting….because he's the IT Manager [P19/B/Int].<br><br>I would report it straight away to the IT Manager, or to my Line Manager. Just immediately alert them to it, and act on anything that I've been requested to do. Yes, just bring people's attention to it straight away I suppose that it's just common sense, really. It's not because there's a specific policy in place, because I know that over the last few months when it's been spoken about quite a lot, the IT Manager has been the go-to guy. I'd probably |

| | | |
|---|---|---|
| then do, but it's not always my next port of call [P6/C/Int]. | I think about it (cyber security), but rely on the fact that we employ a full-time IT Manager to take care of this [P25/B/DS].<br><br>So, I think that possibly the biggest risk for this organisation is that sort of complacent feeling that we pay an external body to do this for us; and, actually, that's really good, but it's only part of the picture. So, I would think that we all need individually to improve how we manage our cyber security [P4/C/Int].<br><br><u>Formal guidance</u><br>So, that got loads of alarm bells ringing because he (Participant 3) has been here for three and a bit months. How could he work for us for thirteen or fourteen weeks without understanding? But, you know, there's a question I'm asking myself: Is it something to do with how we trained him, or is it just that he hasn't got the nouse to really understand these kind of issues? And I think it may be a bit of both [P1/A/Int].<br><br><u>Responsibilisation and Blame</u><br>Which is why he's not here anymore (P3 left the employ of the business the previous day), because he didn't recognise the severity of the thing that he did. He couldn't see why it was a problem. And so, you know, not being able to see why it is a problem is worse than actually doing the deed [P1/A/Int]. | make my Line Manager aware of it. And anyone else in the team who was there, just in case it wasn't only me who was being targeted. And I might speak to one of the Directors of the firm, just to cover my back; that I've made people aware of it [P20/B/Int].<br><br>Well, to be a bit more specific, I don't think that there is a policy written down anywhere – or if there is, I haven't been alerted to it. I think that the obvious thing that people do when they get something suspicious is that they just tell the IT Manager, and he will advise them what to do. In essence, there is almost a way of dealing with it there. But I don't know if there is any sort of formal policy [P21/B/Int].<br><br>I would probably bring it to the attention of my direct boss (i.e. Line Manager), the Head of the Department, who would then, I imagine, report it to the IT Manager. Just because she is higher than me in the hierarchy, I suppose [P22/B/Int].<br><br>I'd get in touch with the IT Manager, and let him know. He would be my first port of call. Just because, I suppose, he's in complete control of all the systems, and he would know how to approach the problem systematically, how to take an organised approach. Whereas, someone else wouldn't have that awareness and knowledge [P23/B/Int].<br><br>I would probably contact the IT Manager…..Because he sends out all these emails about cyber security, and so I just know that he is the guy to go to [P24/B/Int].<br><br>We don't have a formal policy on reporting things….Although, the IT Manager raises it at every board meeting, and just bangs on all the time that we must report to him anything that seems unusual…he repeatedly sends out emails, each week, saying 'everyone look out for this, look out for that'….He always tells us |

| | | |
|---|---|---|
| | | to report to him anything vaguely suspicious. He sent one to us yesterday, saying that, even with what seems to be an internal email, if you are not sure about it then send it on to him without opening it…(He does this) to a tedious extent, I have to say. But I think, actually, it's beginning to sink in [P25/B/Int].<br><br>I think that the IT Manager is the main person that we go to first if there is anything suspicious. I naturally just go to him first. And if he wasn't there…, I'd speak to the HR Manager. I think it's just common sense. I don't want the responsibility of anything going wrong because of me, so I will naturally just do that. I just think that it's common sense, that if the IT Manager isn't there, I would need to find the policy and I would check the Intranet. And if it's not there, then I would need to go to HR. And you just follow a stream. It's not anything that I've been told to do, or I think is right. It's just what I believe is common sense [P26/B/Int].<br><br>Firstly, I would tell the IT Manager, just because he's the IT guy. I don't know how I know to do that. I think it's because he always talks to us about cyber security. So, he would just be the first person I would go to, if I thought there was anything wrong with a particular email [P27/B/Int].<br><br>I base my knowledge of that on a general understanding of what is going on. I couldn't point you towards specific wording in the staff handbook. But I believe the policy would be to immediately stop what I was doing, speak to the IT Manager – either by phone or email – arrange for it to be isolated, and for the necessary steps to be taken. But I think that the policy, which I am going to say is implicit, or that I understand to be what would happen, is: Don't try and do anything yourself; go and speak to the expert. Maybe it's just common sense. But if your question was specifically asking: |

| | | |
|---|---|---|
| | | 'Is there a written policy?', then no, I'm not aware of one. But there is a culture, for want of a better word, in how to deal with this. It's not as if we wouldn't know what to do, but that we would go and speak to the IT Manager, or to *Advance Legal*, who provide our IT support as well [P28/B/Int].<br><br>I think there is something in the office manual, but I'm not sure about that. But the general sort of day-to-day policy is that if there is any hint of a problem, then we refer it to the IT Manager. He'll then look into it. So basically, because we have the benefit of having him here, anything like that we refer to him. Because (he) is very proactive. He's constantly sending us emails with updates, and asking us to keep an eye out for certain things. And in almost every one of those emails, he writes: 'If you have any concerns, anything that you are not sure about, please let me know' [P29/B/Int].<br><br>**Business C**<br>I would contact our IT Support company. And I'm pretty sure that's what all the staff would do: Firstly, because they all know that they are our IT Support; and secondly, because the Office Manager (Participant 10) is the usual conduit. But it also flags up that we probably need to have a policy on it [P4/C/Int].<br><br>I guess, if my Manager was in I would tell her. I guess though, the thing to really do would be to talk to the Office Manager (Participant 10), and then tell the IT Support company. So, pretty sharpish, I'd probably tell as many of them as I could, straightaway [P5/C/Int].<br><br>If it was an email that had come in – and we get lots of junk email anyway – it would be deleted, and that's it [P6/C/Int].<br><br>We have this ISO 9001, under which we are supposed to report |

| | | |
|---|---|---|
| | | things that have gone wrong, or incidences and that sort of thing. And I only generally think to report things to that about 3am, two days later. Normally, I then do, but it's not always my next port of call [P6/C/int].<br><br>I'd contact the Office Manager, because anything related to the office, I would always report it to her. If I'm honest, I think it's because a lot of it is just common sense, because that's what everyone does, just report it to the Office Manager, whatever it is [P7/C/Int].<br><br>Well, we've got Company X as our IT Support. So, we would contact them [P8/C/int].<br><br>First, I would tell my Line Manager (the Office Manager – P10). Then, tell out IT Support company [P9/C/Int].<br><br>In a way though, (if I had received a suspicious email) first I would probably think that everyone will have noticed that the email is really dodgy. If it didn't look *really* dodgy, but I wasn't sure, I *would* contact my colleagues...If I noticed it, I'd be surprised that the others didn't notice it; because I don't know a lot about cyber security [P9/C/Int].<br><br>I'd give the IT Support company a ring…because they would have the answer. They would know the steps to take. Which is what happened with the *Crypto Wall* incident. When I told them what was happening, they said: "Get everyone to log off." It was quite scary [P10/C/Int].<br><br>Stop. Phone up the Office Manager (Participant 10), and then phone up the IT Support company. I wouldn't move any further. I wouldn't switch it off, I wouldn't move anything. I would just leave it there [P11/B/Int].<br><br><br><u>Risk and Work pressure</u><br>I don't ever know whether to click on certain things that come into my junk email box, |

| | | |
|---|---|---|
| | | particularly. Whether it's safe or not. Sometimes I risk it…I don't want to miss anything [P9/C/Int].<br><br><u>Social engineering</u><br>I had one email come through the other day, and it was from our Chief Executive. But it wasn't actually from her. However, it was very well written, and had my first name at the beginning, and then her usual 'kind regards' at the end. The only reason that I became suspicious was that in the middle of the email she asked me to do something that she would never normally ask me to do. So, I deleted it. It was first thing in the morning. It was one of the very first things that I opened that day. And it was just sort of sitting there. And I read it about three times, and concluded that there was no way that she would write a particular sentence in the way that it was written [P9/C/Int]. |

### 3. Framework matrix for the 'Contextual influences on behaviour' theme

| 3.1 Financial | 3.2 Personal | 3.3 Professional | 3.4 Technological |
|---|---|---|---|
| <u>General</u><br>Actually, the corporate work that I do subsidizes the business. So, that's the situation, but that can't go on indefinitely, and so that means that we (the company) are under quite heavy financial pressure the whole of the time [P1/A/Int].<br><br>This business has been losing money ever since I set it up, so I've constantly had to put money into it to keep it going [P1/A/Int]. | <u>General</u><br>I think that if you have a non-technical background, it's difficult to actually think technical [P28/B/Int].<br><br>'[Cyber security] is not something that I take much notice of on a day-to-day basis……<br>I think it depends upon the type of personality that you've got. I try to get on with my day-to-day job. So, I'm quite operational, I think. More operational than strategic. I don't like reading loads of stuff. I like just getting things done. And I think with | <u>General</u><br>I have (just) disseminated it (a new policy) to my department. I don't know whether it has been disseminated to the rest of the staff. We do act in little, rather ad hoc groups within the firm, as I'm sure most businesses do [P25/B/Int].<br><br>We've got our KPIs to do, and that's what we're governed by [P11/C/Int].<br><br>And, you know, when the IT Manager sends | <u>General</u><br>I am in the process of upgrading our internet connection. I have on occasions had to resort to connecting via my phone's 4G network [P1/A/DS].<br><br>Yes, when I was off sick (for 3 months), I logged in and used it (the remote desktop facility) from home on a few days, and it was *so* slow. Frustratingly slow. I mean, not just on sending email, but even when you were using things which you wouldn't normally use the Internet for, such as |

If I had a Ransomware attack now, I would probably close the business….Because this business is dragging itself out of the mire, and it has been for years, really. So, some serious setback could be enough to tip the balance in favour of just wrapping it all up [P1/A/Int].

We are under quite heavy financial pressure the whole of the time. So, writing a cyber security policy doesn't do well in the prioritisation wars with phoning a customer or delivering the service [P1/A/Int].

Cyber insurance

**Recently, the government has begun to urge small and medium-sized businesses to insure themselves against cyber security risks. So, if this business decided to do that, do you think it would affect you in any way?**

In a way, it would make me feel a little bit better. But possibly, I'd be a little less cautious, which wouldn't be a good thing, necessarily……If we were insured, then I might risk it sometimes, if I thought that checking it further would make things awkward and hold things up [P9/C/Int].

Yes, it sounds awful, but I think I would be less worried. Because we've talked about all of these serious consequences, it makes you much more wary, knowing about them. But if you've got that mental security blanket of: 'If it all goes pear-shaped, it's fine.' Which is silly, because it

something like cyber security, it's something that is completely different to my job, and I think it's not something that I spend much time thinking about, because it's not going to improve my performance on a day-to-day basis [P7/C/Int].

If people have my mindset – and I'm sure that a lot of people do – when you're working, you just want to get on with your work, and get on with the job in hand; and often you're obviously not focussing on whether there might be a cyber security issue here or there [P7/C/Int].

It's just that, if someone phoned me and said: 'There's a funny email in your inbox. I've deleted it from my inbox ten minutes ago,' I would not really be concentrating on what they were saying; my day would have moved on. That probably sounds terrible [P9/C/Int].

At the end of the day, everyone wants to follow the procedures [P23/B/Int].

But then, obviously, I don't know how other people work [P23/B/Int].

And I like to think I'm probably a bit more switched on, because I've got a bit of a background in IT sales. And I've gone through all this training here recently. So, I like to think that I'm quite alert to it. Whereas, I would think that quite a lot of my colleagues aren't quite up to the same

round an email about it (a cyber security threat), you sit there and you have a few minutes panic about it. But then we are so busy that that feeling doesn't last all day. You read something, and it makes you think about it. But actually, by the time you've picked up the next file (task) it's almost gone [P12/B/Int].

At the moment, while I am training, I need to be showing that I am valuable, and that I can take on as much as I can. And yes, there is quite a lot of pressure….But I think it all depends upon how much you want to put into it. There are some people who do 9am to 5-30pm, and stop there. For me though, this is meant to be a career, rather than a job. So, it does overlap with your personal life, if you've got certain goals that you want to achieve [P12/B/Int].

Yes, and cyber security is a big part of compliance now. That's one of the sections that they (The Solicitors' Regulation Authority) are looking at. So, you know, we have to make sure that we have policies, and we have to make sure that everybody sticks to them. So, we have no choice, really [P15/B/Int].

Blame

And I always make it very clear that if anything is reported to me (the IT Manager), it's not used as a stick to smack them with. It

typing a *Word* document. It was painful [P6/C/Int].

In the charitable sector, some of the people with whom we communicate are volunteers, and the ability of some of them to word an email in a professional way is limited. So, sometimes their emails can be wrongly thought to be spam because of the unprofessional wording within them [P6/C/Int].

Remote working

I have worked for a number of firms where you actually log in on your computer remotely. Here, we've got no remote working, or we've got it through an *iPad* which doesn't really work, so I've given up on it…It's really limited here. In other firms that I've worked for, you could work from home and be looking at the actual hard drive – the server, not your own hard drive. But here we work on hard drives. It's just not the same as working from a remote server, to which you then log in. In the other places that I have worked, we had formal policies. But here, it's so limited. The IT Manager said that with the *iPad* you have some kind of parallel app. But it was so rubbish, and you had to have the computer on here (in the office, simultaneously). But I've come from a place where you let nobody know your password, you let nobody use your computer, you must never leave it on (logged in) when you

| | | | |
|---|---|---|---|
| would still happen; you'd still go through all those processes and all that stress, and your money going or your reputation. But you would have that sort of mental security blanket [P6/C/Int].<br><br>I guess it would give more of a safety net, if you did do something…I guess that – I don't want to say you wouldn't worry as much about it – but you would probably be more inclined, maybe, to click on that link…..I mean, if you know that it will be fine because we've got insurance, you might be intrigued to see if it is…or not. So, you might just click on it anyway…(And) I kind of think that as an employee – I know that it might sound really bad – that this (being vigilant to cybercrime, and whether you would be more or less vigilant because the business was now insured) is the kind of thing that you wouldn't necessarily think about. I'm just a normal employee, whereas Directors might think like that [P24/B/Int].<br><br>I think it would give me more security, to know that if I did something risky by mistake, then we would have some protection…(but) there is that risk (of complacency), I suppose [P10/C/Int].<br><br>Yes, I think some people could become complacent. But I think that most people would just continue doing what they usually do. At work, I look up stuff more or less just the same as I do at home. So, there's not really any distinction with that. For me personally, I | level. But, I mean, I could easily still be tricked. But I just think that there are probably colleagues who are a bit more naïve than I would be [P21/B/Int].<br><br><u>Blame</u><br>I think that, on the ground level – in the trenches, if you will – there is a very real concern about personal liability, as in: 'Oh God, if I do something wrong, what does that mean?' [P16/B/Int].<br><br><u>Cyber security</u><br>**How much thought, if any, do you give to cyber security within your personal life?**<br><br>I am tech-mistrustful [P17/B/DS].<br><br>I am conscious of it at a general level, but rely on the IT support provider to have downloaded protection on each device [P4/C/DS].<br><br>A bit of thought [P7 and P10/BC/DS] and [P12/B/DS].<br><br>The occasional thought [P23/B/DS].<br><br>Not much [P9 and P11/C/DS] and [P15 and P25/B/DS].<br><br>Some thought [P5 and P6/C/DS] and P13, P14 and P16/B/DS].<br><br>Quite a lot [P8/C/DS] and P18, P20 and P27/B/DS].<br><br>I try to be vigilant [P19/B/DS]. | not a name and shame exercise….You've got to get people to buy in. And you don't do that by slapping round the face with something after they've given it to you. If there is a point place for naming and shaming, it is where somebody is a repeat offender, and is obviously showing no care or consideration for the business, then the naming and shaming goes to their manager, and the process of escalation works from there. But, beyond that, I don't see naming and shaming ever being useful. If anything, it pushes people in the opposite direction to where you want them to be moving [P18/B/Int].<br><br><u>Cyber security</u><br>**How much thought, if any, do you give to cyber security within your working life?**<br><br>I assume that when I am at work that cyber security is already being dealt with by various different softwares that are installed [P24/B/DS].<br><br>Generally, during working hours is it not at the front of my mind; I only think about it if I feel something does not seem right [P9/C/DS].<br><br>I think about it, but rely on the fact that we employ a full-time IT Manager to take care of this [P25/B/DS].<br><br>I rely on the IT Manager to provide the basic protection, and keep my internet cynicism | are physically away from it, and it would shut down. Here, to use the *iPad*, you have to leave your computer on, which would mean that anyone here could use my terminal to access it. And I'm not comfortable with that. That could include a cleaner, or even a client wandering around. Yes, that needs to be much stricter, but we need a proper server system for that [P17/B/Int].<br><br>Originally, I worked at home one day a week, because I lived far away. So, my home PC was set up to work from the network, so that I could work at home (via a remote desktop facility). But since the IT Manager changed our service provider, I can't work on my PC from home. I don't know why, but he hasn't managed to sort that out. So, I have to work on my *iPad*. It is limiting. I mean, I can work on my emails, I can get into my desktop – I've got a parallel thingy – but the thing that concerns me is that if I've got to do a document I have to email it to myself on my home email address, then work on it, and then email it back. Because I can't do major work on my *iPad*….It's a workaround, but it works. It's fine. If I'm drafting a document, I just draft it on my PC, and email it to myself. But that's an additional concern: That I've got documents flying about (in cyberspace) via my Sky.com email account, |

think it would be just the same, really [P7/C/Int].

No, I don't think so. I mean, it probably would – I don't know if it should – but it might give everybody a little bit of reassurance that if something did go horribly wrong then, at least, we would be covered, hopefully. Whether that would make people be a bit less vigilant, I don't know. I would hope not. (But) I think there's a risk (of complacency). I hadn't thought of it, but yes, I think so….I think that with some people there is a chance that they would be less vigilant [P19/B/Int].

Not me personally, because I'd like to think that in Accounts we are probably more aware of the threat than a lot of other people in the firm. But I think that there are some other people in the firm who, if they knew that we were insured, might be more blasé about it, perhaps thinking: 'Oh it's ok; now we're insured'……But we are in Accounts, so we would always be on the lookout for cybercrime [P20/B/Int].

I don't know. I would like to think that it wouldn't make me more casual, but who knows. I imagine there would be – well, insurance has always got conditions to it, hasn't it? – so, there would be things that we must or must not do, in order not to jeopardise the insurance coverage P5/C/Int].

I think it would, because if you weren't to invalidate your insurance you would have to comply with a whole new

I'm very conscious about opening suspicious looking emails, and opening attachments from third parties [P22/B/DS].

In my personal life, I am quite cautious about security [P29/B/DS].

I think about cyber security in my personal life [P24/B/DS].

I give more and more thought to cyber security at home, especially when hearing stories/reports in the media [P26/B/DS].

I don't think of it as a separate issue [P28/B/DS].

<u>Risk</u>
And there are cyber security habits that I have brought from every job that I've had since I was eighteen, which are not always present in people who have been here for 30 years or so. And I think that's a matter of vulnerability [P16/B/Int].

<u>Social engineering</u>
I keep on getting emails purporting to be from the Law Society, which clearly aren't. And the only reason I knew that they weren't is because I got three of the same, one after another. Otherwise, I would have opened it, because I wouldn't have known any different [P25/B/Int].

I had one email come through the other day, and it was from our Chief Executive. But it wasn't actually from

about websites and emails [P17/B/DS].

A little bit of thought [P12 and P22/B/DS].

Less so than in my personal life, as safeguards are already in place [P21/B/DS].

Not much [P6 and P11/C/DS].

Some thought [P5/C/DS] and [P13 and P16/B/DS].

More so since the Crypto Wall incident [P4/C/DS].

Probably more thought that in personal life. It's a constant threat [P18/B/DS].

More than in my personal life. But I'm sure there is room for improvement [P10/C/DS].

More thought than in my personal life, as I receive more junk emails at work [P14/B/DS].

More thought than in my personal life. For some reason, I'm much more careful at work with information [P15/B/DS].

Quite a lot [P8/C/DS] and [P29/B/DS].

I am careful, particularly when we get junk emails; I don't open attachments. Also, I would never allow anyone outside of the business to access the network [P7/C/DS].

Working in Accounts, it is something that we are aware of, and we are as careful as possible [P19/B/DS].

which probably isn't the best thing…[P25/B/Int].

<u>Work/personal divide</u>
I've got two mobile phones (one personal, one work-provided). I don't see it as being a pain. I see it as a convenience, actually. Erm, because it means that I can separate personal life from work life [P2/A/Int].

<u>'Workaround' activity</u>
**So, do you sometimes send work to yourself via your personal email? And do you ever use data sticks for that same purpose?**

I think if people are working on reports and things, then they don't necessarily need to connect in to the network, in order to work on that at home. They have got the document, they might have emailed it to their personal email address, or put it onto a memory stick, and that's probably just as good for them because the remote connection is sometimes just a bit slower [P5/C/Int].

I've sent documents to myself via my personal email. And sometimes I've used a data stick [P6/C/Int].

I have (done both), yes [P7/C/Int].

Very occasionally I've done that (via personal email or data stick). Or the other way I do it is to pop the file that I want on to my desktop, so that I can then work on it offline [P8/C/Int].

| | | | |
|---|---|---|---|
| set of standards that the governance of that insurance would demand to be in place; otherwise, the insurance would be invalid [P8/C/Int].<br><br>That depends on what were the terms of the insurance were. Because if the cyber insurance being valid was dependent upon certain actions, then that would obviously create some extra work or something for me. Other than that, I can't think of anything that would have a direct impact. I suspect that the way that it was communicated and implemented would mean that (complacency) wasn't allowed to happen. And actually, it's one of those things where just because I have car insurance doesn't mean that I go out and crash my car. And I think that it probably makes you more aware of the issue. And I think that, given our experience in having Professional Indemnity insurance, we know how important it is to get something right, and to actually be able to afford the insurance. So, I don't honestly think it would have that impact, no [P16/B/Int].<br><br>It shouldn't do. Just because you have insurance, doesn't mean that you have free rein to click on every link that comes to you. There shouldn't be (a risk of complacency). But it could happen. People might think: 'Oh, it's ok, we're insured' [P27/B/Int].<br><br>Well, I think that, in some ways, it would give protection, in that if something were to | her. However, it was very well written, and had my first name at the beginning, and then her usual 'kind regards' at the end. The only reason that I became suspicious was that in the middle of the email she asked me to do something that she would never normally ask me to do. So, I deleted it. It was first thing in the morning. It was one of the very first things that I opened that day. And it was just sort of sitting there. And I read it about three times, and concluded that there was no way that she would write a particular sentence in the way that it was written [P9/C/Int].<br><br><u>Social media and Risk</u><br>And it would be dead easy to get me, because I do a lot around certain information, all over my *Facebook* page, because I share a lot of information because I've got a big *Facebook* page. So, it would take very little for somebody to know what my interests are. And if they then copied one of the names that I'd been following, I'd open it (an email)….Anybody sending me an email around funding or women's issues, straight off I'd open it [P11/C/Int].<br><br><u>Technology</u><br>I am nervy about computers. I love them, but I am very nervy about them, because I think that we are ignorant to the power that they have, or how people can use them[P11/C/Int]. | I always try to stay vigilant, and look for anything that might be suspicious [P26 and P28/B/DS].<br><br>Our IT Manager is always keeping us up to date with the latest scams etc., so I am constantly thinking about it [P27/B/DS].<br><br><u>Formal guidance</u><br>**Do you think that more formal policy on cyber security might interfere with your ability to do your job?**<br><br>**Business A**<br>I guess that depends on how much formal policy is given, and how [P1/A/Int].<br><br>No, I don't think so. It would just add more peace of mind, if anything; that what you're doing is correct, and in accordance with the rules. Rules are there for a reason [P2/A/Int].<br><br>**Business B**<br>No. I don't think it would have any effect, really [P22/B/Int].<br><br>No, I don't think so. I think it's just a different way of working, isn't it? You know, we now check Bank details – yes, it takes two minutes longer, but it's not that bad [P13/B/Int].<br><br>I think it can be done, and I think that, as soon as you have adjusted to it, it doesn't actually affect your time balance, because you are already used to it; it's just that easing into | Yes (I have done both) [P9/C/Int].<br><br>Yes. That's the sort of thing that people do here [P10/C/Int].<br><br>Yes (I do both). I don't use data sticks very often, though [P11/C/Int].<br><br>I think I've done it once or twice. I've sent work to my personal email, and then picked it up at home, without having to borrow a work laptop from Participant 18 [the IT Manager] which is all set up properly for remote working. But actually, if you are just wanting to look at a couple of documents over the weekend, it is quite easy just to email it to yourself [P12/B/Int].<br><br>I probably would, yes. That's the long and short of it. I'd take it from my private email address, and I'd email it to my work one. You know, aside from me sitting down at my PC or may laptop at home, that's the way I'm going to do it. So, unless you have the system on that…You know, it needs to be everywhere if it's anywhere [P16/B/Int].<br><br>If I've got to do a document (at home), I have to email it to myself on my home email address, then work on it, and then email it back. Because I can't do major work on my *iPad* [P25/B/Int].<br><br>There was one occasion when I needed to stay with my Mother, and there were a couple of |

| | | | |
|---|---|---|---|
| happen, then the insurance company would pay out to rectify the situation, which is reassuring. Without it, there is always the risk that something happens, and the firm goes bust trying to pay for it. So, I guess, in that way, I would feel more protected. I guess that there is the potential for (complacency). But, in the same way that we have professional indemnity insurance, you don't want to find yourself in a position where you haven't used your common sense or your due diligence, and then the insurance company refuses to pay out. So, not personally, but perhaps there is the potential for complacency [P29/B/Int].<br><br>No, I don't think so….(but) I could see how some people might become a bit complacent, knowing that. But I don't think that I would, because I can't see how being insured against it stops it, just because you are now insured [P26/B/Int].<br><br>I don't think so. I think it would make people feel a lot more vulnerable, because rather than it being a possibility, as soon as you get insurance for something it is almost like you're accepting that, whilst it's not inevitable, it is a higher possibility than it would be if you didn't have insurance, if that makes sense? So, I think it would make everyone a bit more switched on, a bit more alert. I don't think the people here would become complacent. But then, obviously, I don't know how other people work. | | it stage…And people need to know that a policy is achievable; that they actually can do it, and incorporate it into their day. Whereas, if it's thrown in or launched too quickly, then it's immediately going to cause friction [P23/B/Int].<br><br>I don't think so. I think that everybody needs to be on board. And I think that if it makes our jobs a bit slower – which it might do, if there are extra checks and stuff to do – then, at the end of the day, it going to be more efficient because it's going to be done properly [P19/B/Int].<br><br>No. Initially, it would take up more of my time, because I would be having to learn something. But once I had got that information, it would probably save time, because I would be aware of what to look out for, what I should and shouldn't do, and so on [P26/B/Int].<br><br>I hope not, because I hope that we're doing what we can for cyber security, anyway. It would just set in stone what we do anyway. So, I hope not. My Job is already made more difficult by the amount of compliance we have anyway. And the fact that I am one of the Compliance Officers, who then has to report on people, makes it even worse. So, I don't think it would change what I do [P15/B/Int].<br><br>No, provided that the steps that we take are not going to interfere | things that I needed to do – you know, some lengthy reports – so, I emailed the information to myself, but it didn't have any client information in it [P29/B/Int].<br><br><u>Remote working and Risk</u><br>My son's laptop is very slow, maybe because it has too little memory, but it also seemed to be running some Windows anti-malware that was eating up a lot of the computer's resources. So, I searched a few Windows user forums to find ways to disable Windows Defender, which seemed to be the culprit. This improved the performance a bit [P1/A/DS].<br><br>But sometimes my boyfriend uses it (my laptop at home) [P6/C/Int].<br><br>There's three of us who use it (laptop at Home). Also, my Mum works from home on it as well [P9/C/Int].<br><br>Me and my husband use it (the laptop that I sometimes do work on at home) [P11/C/Int].<br><br><u>Social engineering and Risk</u><br>But also my emails are copied to my secretary. And she opens my emails…….And even the ones that are not copied are often accessible by others. For example, I have access to the email boxes of all the people in my department, and they have access to mine. So, somebody else could open an |

| | | | |
|---|---|---|---|
| It depends on how you perceive it really, I suppose. But in relation to the earlier scenario, nobody would want to be responsible for that kind of situation. And I think that, anyway, that would put people off. And once you felt that you were in a position where, potentially, you could be responsible – you could open an email, and click on a link – seeing as the insurance would be there, all I think it would do is to increase people's alertness. And they would think: 'Ok, this is a serious risk now, and I could do this and impact the business in this way'….(Although) I do think that it could work in two ways. People could become complacent. But I think that people do think of it as a business, but at the same time they also think of what they personally contribute to the business. And I don't think that anyone would want to contribute negatively, especially with something like that. I do think, especially here in this business, it would increase people's awareness. As I said, I think that a lot people don't think about it (cyber security) that often, and I think that if that was put in place they would think seriously about it [P23/B/Int].<br><br>I don't think it would. I mean, we hold professional indemnity insurance, and it doesn't take away the fact that you could still be sued for professional negligence. It's a bit of a safety net, if the worst comes to the worst. And the same with cyber insurance. It's not going to change the fact that we can be | | with work activity. For example, we have to be aware of the client account details. If procedures were put in place which added two or three hours work to each file, because certain things had to be done – I can't think of a specific example – that could potentially slow it up. But I really can't see that being an issue. We always work to adapt. It's simply part of everyday life [P28/B/Int].<br><br>Yes. But I don't see that as a problem….Yes, it will slow some things down, but actually in the long run it can speed things up [P17/B/Int].<br><br>Not the standard (of my work), but perhaps the efficiency. I mean, it would be slower, but obviously it would be safer [P27/B/Int].<br><br>I suppose it depends. You could see a situation where all emails have to go through somebody before you are allowed to view them, which then would obviously hold things up, because I'm sure that the business, as a whole, gets a lot of emails each day. So, yes it would depend…… not spending loads of time ticking boxes, or whatever [P14/B/Int].<br><br>It depends on their content. We're already in quite a heavily regulated industry, and I think it puts quite a lot of people off. Because there are definitely aspects of this job where you feel like you are just doing | email. So, we all need to be vigilant [P25/B/Int]. |

| | | | |
|---|---|---|---|
| attacked, it just means that there is a bit of a safety net if that happens. Given the way that we think about it, I don't think that it would really change anything [P12/B/Int].<br><br>No, I don't think so. We are used to being insured against other risks – through Professional Indemnity insurance, for example – so, it would be just more of the same kind of thing [P25/B/Int].<br><br>No, it shouldn't do. I can't see how you can get insurance. One of the things about insurance is that it is monetarily limited. And if you are a small enterprise which may affect a big enterprise, would you have unlimited insurance? I mean, it would just be phenomenally expensive. It's just seems like a great government idea, without actually being thought through; it doesn't actually do anything….(and even if you have cyber insurance) You shouldn't tell the employees. If it's just the business owners and the IT Manager that know about this sort of thing, and it's just a backup, that's ok. But really, I can't see that an insurance company could actually provide you with the right insurance, because it's just so brand new, and you'd just be wasting your money. And if you tell the staff that you've got insurance, then you really are taking a big risk there [P17/B/Int].<br><br>No. I would hope that people wouldn't just think: 'Oh well, they've got the insurance, so it | | compliance more than anything. And you kind of think that your job is just going to become compliance; that you will not actually be doing your job most of the time [P21/B/Int].<br><br>It depends what it said. It could do [P25/B/Int].<br><br>Possibly. I think it does play on your mind a lot more than it used to. And you would be more inclined to double or triple-check things, to make sure that you are not being targeted. But, you'd rather that than get something wrong. It might slow things up a bit, but it's better practice to do that [P20/B/Int].<br><br>Possibly. I think it would mean that we'd have to spend more time. So, potentially our workloads could increase, if we are having to make more checks on a file [P12/B/Int].<br><br>I think that if there were more policies that I had to follow, it would probably slow me down a little bit. I'd have to be consciously thinking all the time: 'Am I doing this right? Am I following this policy correctly?' So, I guess to a certain extent it would, yes [P24/B/Int].<br><br>In some ways, I think that it feels as if you are having more pressure put on you, when it's a very formal process [P14/B/Int].<br><br>Yes, I have huge concerns about it. Because if you go for an over-zealous approach……I mean, | |

| | | | |
|---|---|---|---|
| doesn't matter' - because an insurance company will try to find any reason not to pay out.<br>Obviously, if we can get it, and it works for us, then we'd have it. But (as a Director of the firm) I wouldn't want to make a big thing of it to the staff, and say: 'Don't worry, we're insured, ' because I think it would put it more to the back of people's minds [P13/B/Int].<br><br>No, not really. You would still have to be as vigilant because the insurance company would no doubt word the agreement in a way that they could still investigate whether you were to blame or not. With any kind of insurance, you still have to take some care…It's like when you're driving; you don't suddenly think: 'Oh, I've got insurance, no problem' [P14/B/Int].<br><br>It makes you feel slightly better that you've got it, I suppose. It depends how much it costs as well, doesn't it?<br>I wouldn't think (it would bring a risk of complacency), because we have reminders (via email) several times a day that we have to be vigilant. So, I think that the fact that we had cyber insurance would make no difference whatsoever, because we would still continue to get all of those daily reminders [P15/B/Int].<br><br>No, I don't think so. I would like to think that I would be careful, regardless of that [P22/B/Int].<br><br>No. For me, it's exactly the same as Health & Safety. You know, would you become complacent | | you've got to weigh the balance out [P16/B/Int]<br><br>Yes. I mean, it's starting to feel as if the job is more like a procedure checklist [P29/B/Int].<br><br>**Business C**<br>I think it would probably help, actually [P10/C/Int].<br><br>No. Having more policies and procedures to follow may take up a bit more time, but I think once you learn something, it's laid out, you call it up, and then you follow it. So, in a way it's easier than trying to make a decision, and maybe then going the wrong way [P9/C/Int].<br><br>No. Something like this should just be fitted in, with regular updates, so that we're all aware of it. Keeping it workable, that would be the answer, so that we do it all the time. Keeping it workable. And, you know, it could be something that flashes up on our screens every morning when we turn our computers on [P11/C/Int].<br><br>No, I would hope not. It might take a little more time, but it would be worth it [P5/C/Int].<br><br>Hopefully not. As I said, it depends on how much extra time in your working day it took up [P7/C/Int].<br><br>Possibly. It depends upon the amount [P6/BC/Int]. | |

| | | | |
|---|---|---|---|
| if you saw a risk (for which you have insurance)? No [P11/C/Int].<br><br>I think it (cyber insurance) would be a very sensible move. And I certainly think that part of the requirements of the insurance would be that we all had to attend training. If, after the training, somebody did something which was contradictory to what was told in the training – for example, always scan your attachments before you open them – if somebody doesn't do that, then obviously the insurance probably wouldn't pay out. But I think insurance is definitely a way forward. We use it in my own department – Commercial Property – for indemnities. So, I can see that, in terms of our day-to-day practice, that it would probably include training, but I imagine that this would be subsumed into the overall workload, without being too onerous [P28/B/Int].<br><br>It's funny. Yesterday, I had this discussion about cyber insurance, and I don't think it's a question of should we or shouldn't we? I think it's a question of how quickly can we? [P18 (the IT Manager)/B/Int]. | | It could do. But I think then the key would be making sure that we write policy that is practicable and useful. It's how we write it, and how we apply it [P4/C/Int].<br><br>It could do [P8/C/Int].<br><br><u>Informal guidance</u><br>**Informally, have you ever received any advice on cyber security from any of your work colleagues?**<br><br>I was told not to allow the web browser to save passwords [P6/C/DS].<br><br>I was told by a colleague to ensure that I don't open spam attachments [P7/C/DS].<br><br>Yes, an email came in and we were suspicious of it, and I was advised to delete it [P8/C/DS].<br><br>Yes, in conversations with our IT Manager about the current issues in cyber security, and how to spot dodgy emails, and discussions with other colleagues [P13/B/DS].<br><br>Sometimes, people will mention it if they have received an email that doesn't look right, and ask if anyone else has received the same or similar [P14/B/DS].<br><br>Yes, yesterday. All to do with people calling us pretending to be from our Bank, to get information to enable them to access our accounts [P19/B/DS].<br><br><u>Informal guidance</u><br>**Informally, have you ever given any advice** | |

| | | | |
|---|---|---|---|
| | | **on cyber security to any of your work colleagues?**<br><br>I wouldn't dream of it! [P4/C/DS].<br><br>Yes, recently I remember advising a colleague about how spam emails often pretend to be from Yahoo, Barclays Bank or whatever, but you can check them by hovering over the address [P5/C/DS].<br><br>Yes, to say, when asked, that I thought that was a dangerous email [P8/C/DS].<br><br>No, I do not know enough to be able to advise others [P9/C/DS].<br><br>Yes,…on how to use safe passwords. Also, giving information about dealing with spam emails [P10/C/DS].<br><br>Yes [P11/C/DS].<br><br>Yes, concerning the checking of bank details received via email [P13/B/DS].<br><br>Yes, when I have been sent a suspicious email and not opened it, I have advised others not to do so [P15/B/DS].<br><br>If I have, it would be mostly to be wary about dodgy emails and links [P16/B/DS].<br><br>Yes, about opening junk mail or spam mail attachments [P18/B/DS].<br><br><br><u>Risk</u><br>I also think that the number of high level part-time workers that | |

| | | | |
|---|---|---|---|
| | | we have creates an air of vulnerability. If someone wanted to target us, it would be very easy for them to say: 'Oh, I spoke to X.' And if X is gone for the rest of the week, and it's Wednesday lunchtime and they are speaking to Y, then that gives credibility from X, which could enable them to get in [P16/B/Int].<br><br>But we are in Accounts, so we would always be on the lookout for cybercrime [P20/B/Int].<br><br><u>Social engineering</u><br>But also my emails are copied to my secretary. And she opens my emails…….And even the ones that are not copied are often accessible by others. For example, I have access to the email boxes of all the people in my department, and they have access to mine. So, somebody else could open an email. So, we all need to be vigilant [P25/B/Int].<br><br>I think you would never forget it (if you were tricked into clicking on something). You would be very careful about how you functioned, and what you did. And it could potentially put you off working in an environment like this, where the risks are quite high. You know, if you've done it once, and you've managed to retain your job, it could have a big impact upon your confidence and how you do things….(And) it could create a bit of an | |

| | | | |
|---|---|---|---|
| | | awkward environment to work in [P12/B/Int]. | |

## Appendix J Recruitment Advert.

# An invitation to participate in, and benefit from, some free University research into cyber security

## Do you give your employees any advice on cyber security?

## How easy is it for them to follow that advice?

## Would you like to find out, in confidence, for free?

**Within the climate of increasing pressure and responsibility for cyber security, businesses need all the help they can get; particularly SMEs, in their understandable struggle to meet the financial costs that cyber security can bring. Yet not all useful advice and support comes with a price tag. This research will assist SMEs by providing the participating businesses with more detailed knowledge of how their cyber security advice works in everyday practice. A key part of this study will be exploring how employees engage with that advice, and identifying cost-free or cost-effective ways to further improve it, strategically and operationally. The anonymity of the businesses and each of their employees will be guaranteed throughout and beyond the study.**

**After the research study has been conducted, participating businesses will each receive a report which contains:**

- **Valuable information on the quality and usability of their cyber security advice.**
- **Employees' feedback – given anonymously and freely – on how easy it is to follow that advice everyday.**
- **More knowledge on identifying and reducing cyber security risks to their business, in cost-free or cost-effective ways.**

**Participation in this research will also help businesses to better prepare for the strong governmental push of cyber insurance as part of the cyber security responsibilities of UK businesses, particularly within the SME sector.**

The study will involve about 8 employees (from each SME) who make use of Internet-linked devices for work purposes on business premises, at home, and elsewhere (i.e. mobile working). For 5 days only, at the end of each day they will spend about 15 minutes answering questions in an electronic diary (clicking some options, and typing some answers). Soon after, they will each be interviewed at a time and place of their choosing. This could be at work (if they and their employer agree to it), or outside of work (if they would prefer this).

**To register your interest, please email Neil MacEwan (PhD Researcher at the University of Southampton) at nfm2g13@southampton.ac.uk** I can then tell you more about me (e.g. my research and career background), and about the project (e.g. what types of question I will be asking the employees during the Diary Study and Interviewing stages of this research project).

# Appendix K Participant Information Sheet.

## Participant Information Sheet

**Study Title**: The everyday challenges of working and 'living' securely in cyberspace.

**Researcher**: Neil MacEwan **Ethics number**: 13250

**Please read this information carefully before deciding to take part in this research. If you are happy to participate, you will be asked to sign a consent form.**

**What is the research about?**
In the UK, there has been a lack of independent research into the everyday cyber security experiences, habits and practices of people who use cyberspace in their working and private lives. This research will help to fill that knowledge gap. I am a PhD student, and this is a piece of independent research, fully funded through the Web Science Doctoral Training Centre at the University of Southampton. Therefore, it carries no risk of financially influenced bias (e.g. through commercial backing).

**Why have I been chosen?**
You have been invited to take part in this research because you are an employee of a small or medium-sized enterprise (SME), and you form part of a modern mobile workforce (i.e. using cyberspace for work and non-work purposes in different physical settings, such as the office, at home, and elsewhere). If you choose to take part, you will be one of about 20 participants in this research, each of whom works for one of three SMEs.

**What will happen to me if I take part?**
There will be two stages of participation. Prior to Stage 1, I will conduct an initial observation of the layout of your office environment at work. This will be done as quickly and unobtrusively as possible. It will simply involve me taking a few photos of the room/office environment, in order to produce a plan of that working environment and a description of the technologies used within it. If you do not want to feature in any photos of those settings, that is fine; I will always ask your consent before taking any photo of your office environment. The photos will only be used as a reminder for making that plan, and will be deleted permanently once it has been drawn up. The plan will never be used in a way which might undermine your anonymity.

**Stage 1** – This will involve answering questions at the end of each day, for five consecutive days. It will be conducted online, via the University of Southampton's *iSurvey* platform. This daily task will take you about 15 minutes, and can be done either towards or after the end of your working day. Each day at 4pm, I will email you a link to that day's questions. Ideally, you should answer all nine of the daily questions in one sitting. But if you need to pause for some reason, and want to return later that evening to complete the remaining questions, you can do so by clicking the 'Save and Quit' button (not the 'Save and Finish' button). This will then generate for you a username and password which you will need to regain entry to the questions later on. The *iSurvey* platform will give you the option of sending that username and password to yourself via email. I suggest that you take that option (rather than writing down on paper what could be a rather long username and password). Later, when you access that email that you've sent to yourself, you will see that it contains a link to the questions and your username and password to regain entry. When you click on the link, you will see that the system enters the username for you, but you must then cut and paste the password from your email into the space provided on *iSurvey*.

**Stage 2** – A few weeks after you have completed this Diary Study, I will interview you for about 30 minutes, at a time and place of your choosing. This will be a confidential interview with me, in which I will ask you some further questions about your diary entries and some related issues.

**Are there any benefits in my taking part?**
By participating in this research, you will contribute to improving the daily online experiences of people in the UK, at home, at work and across/between those converging contexts.

**Are there any risks involved?**
In the absence of safeguards, there would be a risk that your employer might be able to find out the contributions that you made to the research (i.e. via the Diary Study and in Interview). But I will use several layers of protection to ensure that this could not happen (please see the details of this strong protection in my answer to the next question).

**Will my participation be confidential?**
During discussions with your employer(s) in the recruitment stage for this research, I made them aware of the strong condition laid down by my University's research ethics committee that this research should be used for collective progress, not the highlighting of individual practices. In turn, each employer accepted this condition, unreservedly. You can rest assured this work will be conducted in strict accordance with the University of Southampton's policy on research ethics. Your anonymity will be guaranteed throughout and beyond the study, your continued participation in the study will be based on informed consent, and all of the (anonymised) data collected from the study will be stored securely (i.e. data coded and kept on a password-protected computer). As a piece of independent research, this study will be conducted impartially and respectfully towards all of its participants, employees and businesses alike. Your name will never be used or disclosed during, or after, the study. You will be given a personal ID number. I will be the only person who can link those numbers to people's names, and I will never disclose that information. It will be stored securely, and disposed of (e.g. via electronic deletion or document shredding) as soon as it is no longer needed. The businesses will also be given anonymity. Each business will be told that two other businesses will also be participating in the research study, but not which businesses. And they will only ever be referred to by their anonymous participating ID (e.g. Business A). Again, I will be the only person who can link the participant numbers to the businesses' names, and I will never disclose that information.

**What happens if I change my mind?**
Your participation in this research would be truly voluntary. If you wanted to, you could withdraw from this research project at any time of your choosing, without your legal rights being affected.

**What happens if something goes wrong?**
In the unlikely case of concern or complaint, you would need someone to contact who is independent of this research project. That person will be the Head of Research Governance at the University of Southampton (Tel: 02380 595058; Email: rgoinfo@soton.ac.uk ).

**Where can I get more information?** If you would like any more information on this research project, please do not hesitate to contact me (Neil MacEwan) via email at nfm2g13@soton.ac.uk or my Principal PhD Supervisor (Dr. Craig Webber) at C.Webber@soton.ac.uk

## Appendix L Consent Form.

# CONSENT FORM

**Study title:** **The everyday challenges of working and 'living' securely in cyberspace**

**Researcher name:** **Neil MacEwan**

**Ethics reference:** **13250**

**Please initial the boxes if you agree with the statements:**

I have read and understood the *Participant Information Sheet* (04/12/14 – Version No.2) and have had the opportunity to ask questions about the study. ☐

I agree to take part in this research project, and agree to my data being recorded and used for the purpose of this study. ☐

I understand that my responses will be anonymised in research reports of the research. ☐

I understand that my participation is voluntary and I may withdraw at any time without my legal rights being affected. ☐

**Data Protection**

**I understand that information collected about me during my participation in this study will be stored on a password protected computer and that this information will be used only for the purpose of this study.**

**Name of participant (print name)**…….

**Signature of participant**…….

**Date**…….

# Appendix M Diary Study Questions.

On each of the five days of the Diary Study, the participants were asked 9 or 10 questions. These were a mixture of some **Repeated Questions** (questions asked on each of the five days) and **Bespoke Questions** (questions asked only one occasion).

**Repeated Questions**

1. Please type in your **personal ID number**.

   I will have sent this to you via email before the start of this study.

   If you encounter any problem with this, or anything else, in your completion of this study, please feel free to email me for help at nfm2g13@soton.ac.uk

2. During the last 24 hours, which Internet-linked devices did you use for work purposes, **and** what were those purposes?

   When listing the devices, and the work purposes for which you used them, **please specify** whether each device was your own or was work-provided (e.g. my work PC, my own smartphone, my home PC, my work laptop, etc.).

3. During that time period, in which contexts (**office**, **home** or **elsewhere**) did you use those devices for those work purposes (e.g. my smartphone in the office and elsewhere, my work laptop at home, etc.).

**Bespoke Questions**

**Day 1**

4. During all the time that you have worked for this business, have you encountered any problems in your use of the (Internet-linked) **work-provided devices**?

   Examples might include **difficulty**, **frustration** or **slowness** in: a) logging in b) using operating systems and software c) using the Internet d) using work-based email.

   Please name the device(s) on which you encountered the problem(s) (e.g. my work PC), and **be specific** about the nature and form of the problem(s).

5. If you have ever encountered problems on those **work-provided devices**, did you do anything to solve, lessen or work around those problems?

   Please explain **specifically** what you did, and whether by doing it you were seeking to **solve**, **lessen** or **work** around the problem(s).

6. Either on your **personal devices** or **work-provided devices**, during all the time that you have worked for this business, have you encountered anything that you thought was a **potential** threat to either **your own** or **the business's** cyber security?

   Examples mights include: a) suspicious messages via email or social media, perhaps containing links or attachments b) unexpected requests for personal data or security data (e.g. password) c) suspicious looking websites d) suspicious looking pop-up windows within websites or on social media platforms.

7. If you encountered any such **potential** cyber security threats, what action, if any, did you take?

   Examples might include: a) ignoring them b) or doing something more directly in response to them, such as deleting suspicious messages and requests c) and/or reporting them to someone.

8. During all the time that you have worked for this business, have you known of any **actual** threat to **the business's** cyber security that has occurred (i.e. any cyber security incident)?

   Examples mights include: a) individual devices, or computer networks, becoming infected/corrupted by malicious activity/software b) systems, services or applications being disrupted by malicious activity/software c) unauthorised access to, or modification of, data held by the business.

9. If you own a PC or laptop or tablet (i.e. that is not work-provided), is the personal firewall in its operating system (e.g. Windows 7) turned on? If you are unsure, would you know how to check this (without first asking someone or googling for instructions)?

   As with all of these questions, please be honest in answering. I will be the only person who knows your answer (and I will not reveal it, nor its source). Thank you.

10. On that/those device(s) that you mentioned in the previous question, is your chosen Web Browser (e.g. Internet Explorer) set to block: a) third party cookies, and b) pop-ups? If you are unsure, would you know how to check this (without first asking someone else or googling for instructions)?

    Again, please feel free to be completely honest in your answer. Thank you.

**<u>Day 2</u>**

4. During all the time that you have worked for this business, have you encountered any problems in the use of your (Internet-linked) **personal devices**? (ie. those that are not work-provided).

Examples might include **difficulty**, **frustration** or **slowness** in: a) logging in b) using operating systems and software c) using the Internet d) using work-based email.

Please name the device(s) on which you encountered the problem(s) (e.g. my home PC), and **be specific** about the nature and form of the problem(s).

5. During all the time that you have worked for this business, for which **work purpose** have you most often used each **personal device**? (i.e. when listing each personal device, please mention the work purpose for which that device has been most used).

6. How much thought, if any, do you give to cyber security within your **personal life**?

7. How much thought, if any, do you give to cyber security within your **working life**?

8. Are each of the devices that you (ever) use for work purposes password-protected?

   (Please list all of the devices, specifying for each of them whether they are personal devices or work-provided devices, and whether or not they are password-protected).

9. For each of those devices that are password-protected, where and how have you stored a copy/reminder of the password (in case you forget what it is).

**Day 3**

4. Do you use Social Media in your **personal life**? If so, which?

5. Do you use Social Media in your **working life**? If so, which? And for which work purposes do you use them?

6. Does the business that you work for have a policy on employees' use of Social Media?

   If you do not know, please simply state that you do not know (rather than asking someone else or trying to find out in some other way).

7. In your **personal life**, do you use any file-syncing services (e.g. Dropbox, iCloud, OneDrive, SugarSync). If so, which?

8. In your **working life**, do you use any file-syncing services (e.g. Dropbox, iCloud, OneDrive, SugarSync). If so, which, and for what work purposes?

9. During all of the time that you have worked for this business, has it provided you with any guidance on, or training in cyber security (also known as IT security)?

If so, please specify:

a) in what form it was delivered to you (e.g. written, verbal, visual)

and b) whether it was provided by (someone in) the business itself, or by another organisation/person.

**Day 4**

4. During all the time that you have been employed by the company, please list all of the ways in which you have sent work (in digital form) to yourself, for you to work on **remotely** (i.e. away from the office).

   Examples might include:

   a) sending documents/files (as attachments) to yourself via your work email or personal email accounts (this would include using your work email account to send an email attachment to your personal email account).

   b) sending documents/files to yourself via a file-syncing service (e.g. Dropbox, iCloud).

   c) transporting documents/files with you via flash memory drives (data sticks), CDs, DVDs, or removable hard drives.

5. Do you have a wireless (WiFi) network at home?

6. When away from the office or home, do you ever use free, public wireless (WiFi) networks?

7. Does the business that you work for have a remote working policy?

   If you do not know, please simply state that you do not know (rather than asking someone else or trying to find out in some other way). Thank you.

8. Are each of the work-provided devices and personal devices that you have mentioned during this study protected by anti-virus software?

9. Within the business that you work for, who is responsible for ensuring that on all of the work-provided devices the operating systems, key applications (e.g. web browsers and email programs) and security applications (e.g. firewalls and anti-virus software) are kept up-to-date?

   If you do not know, please simply state that you do not know (rather than asking someone else or trying to find out in some other way). Thank you.

**Day 5**

4. When you receive messages which contain links (e.g. via email), do you ever check the validity of the links before clicking on them?

5. When your are visiting websites, do you ever check the validity of their sources (to determine whether they are spoof websites)?

6. **Informally**, have you ever **received** any advice on cyber security (also known as IT security) from any of your work colleagues?

   If so, please mention the most recent occurrence of this, and describe the aspect of cyber security with which it was concerned (please do not name the person from whom you received the advice).

7. **Informally**, have you ever **given** any advice on cyber security (aka IT security) to any of your work colleagues?

   If so, please mention the most recent occurrence of this, and describe the aspect of cyber security with which it was concerned (please do not name the person to whom you gave the advice).

8. Does the business that you work for have a formal policy/procedure for **reporting** risks and incidents which (are thought to) have either threatened or breached the company's cyber security (aka IT security)?

   If you are unsure whether there is such a formal policy/procedure, then please simply state that (rather than asking someone else, or trying to find out in some other way). Thank you.

9. Do you ever feel that your ability to do your job is hindered by cyber security considerations, rules or practices?

10. Do you know whether the business that you work for is insured against cyber security risks?

    If you are unsure, please simply state that (rather than asking anyone else, or finding out in some other way). Thank you.

# Bibliography


Abawajy, J. (2014) User preference of cyber security awareness delivery methods. *Behaviour & Information Technology*, 33(3), 236-247.

Adams, A. and Sasse, M.A. (1999) Users Are Not The Enemy: Why users compromise computer security mechanisms, and how to take remedial measures. *Communications of the ACM*, 42(12), 41-46.

Adams, A. and Blandford, A. (2005) Bridging the gap between organizational and user perspectives of security in the clinical domain. *International Journal of Human Computer Studies*, 63, 175-202.

Ajzen, I. (1991) Theory of Planned Behaviour. *Organizational Behavior and Human Decision Processes*, 50(2), 179-211.

Alaszewski, A. (2006) *Using Diaries for Social Research*. London: Sage.

Albrechtsen, E. and Hovden, J. (2010) Improving information security awareness and behaviour through dialogue, participation and collective reflection: An interventional study. *Computers and Security*, 29(4), 432-445.

Alloway, T. and Kuchler, H. (2014) Attacks spur surge in cyber insurance sales. *Financial Times*, 16 January. Available from: https://www.ft.com/content/94358fee-7d55-11e3-a48f-00144feabdc0#axzz2vxLRckpX [accessed 1 September 2017].

Allport, G.W. (1942) *The Use of Personal Documents in Psychological Science*. New York: Social Science Research Council.

Amir, M. (1971) *Patterns in Forcible Rape*. Chicago: University of Chicago Press.

Anderson, R. (2016) Met police chief blaming the victims. *The Times*, 10 April. Available from: https://www.lightbluetouchpaper.org/2016/03/28/met-police-chief-blaming-the-victims/#comments [accessed 1 September 2017].

Bada, M. and Sasse, M.A. (2014) Cyber Security Awareness Campaigns: Why do they fail to change behaviour? *Global Cyber Security Capacity Centre: Draft Working Paper*. Available from: https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Awareness%20CampaignsDraftWorkingPaper.pdf [accessed 1 September 2017].

Barnes, B. (1981) On the conventional character of knowledge and cognition. *Philosophy of the Social Sciences*, 11, 303-333.

Barnes, B. (1982) *T.S. Kuhn and Social Science*. London: Macmillan Press.

Barnes, B. (2001) Practice as collective action. In Schatzki, E., Knorr Cetina, K. and Von Savigny, E. (eds.) *The Practice Turn in Contemporary Theory*. London: Routledge, 17-28.

Barnes, B., Bloor, D. and Henry, J. (1996) *Scientific Knowledge: A Sociological Analysis*. London: Athlone.

Bauman, Z. (2006) *Liquid Fear*. Cambridge: Polity Press.

BBC News (2016) Talk Talk profits halve after cyber attack. *BBC News*, 12 May. Available from: http://www.bbc.co.uk/news/business-36273449 [accessed 1 September 2017].

BBC News (2016a) Talk Talk fined £400,000 for theft of customer details. *BBC News*, 5 October. Available from: http://www.bbc.co.uk/news/business-37565367 [accessed 1 September 2017].

BBC News (2017) Lloyds of London CEO: Cyber insurance cost to double. *BBC News*, 17 July. Available from: http://www.bbc.co.uk/news/av/business-40629228/lloyd-s-of-london-ceo-cyber-insurance-cost-to-double [accessed 1 September 2017].

Beautement, A., Sasse, M.A. and Wonham, M. (2008) The compliance budget: Managing security behaviour in organisations. In *Proceedings of the 2008 workshop on new security paradigms*. New York: ACM Press, 47-58.

Beautement, A. and Sasse, M.A. (2009) The economics of user effort in information security. *Computer Fraud & Security*, 10, 8-12.

Beautement, A., Becker, I., Parkin, S., Krol, K. and Sasse, M.A. (2016) Productive Security: A scalable methodology for analysing employee security behaviours. *12th Symposium On Usable Privacy and Security (SOUPS)*, 22-24 June, Denver, Co., USA. Available from: https://www.usenix.org/system/files/conference/soups2016/soups2016-paper-beautement.pdf [accessed 1 September 2017].

Beck, U. (1992) *Risk Society: Towards a New Modernity*. London: Sage.

Bennett, S. (2008) The 'Digital Natives' Debate: A Critical Review of the Evidence. *British Journal of Educational Technology*, 39(5), 775-786.

Besnard, D. and Arief, B. (2004) Computer security impaired by legitimate users. *Computers and Security*, 23, 253-264.

Bloor, D. (1982) Durkheim and Mauss Revisited: Classification and the Sociology of Knowledge. *Studies in the History and Philosophy of Science*, 30, 81-112.

Bloor, D. (1992) Left and Right Wittgensteinians. In Pickering A. (ed.) *Science as Practice and Culture*. Chicago: University of Chicago Press, 266-282.

Bloor, D. (1997) *Wittgenstein, Rules and Institutions*. London: Routledge.

Bloor, D. (1998) Changing Axes: response to Mermin. *Social Studies of Science*, 28, 624-635.

Bloor, D. (2001) Wittgenstein and the priority of practice. In Schatzki, E., Knorr Cetina, K. and Von Savigny, E. (eds.) *The Practice Turn in Contemporary Theory*. London: Routledge, 95-106.

Blythe, J.M., Coventry, L. and Little, L. (2015) Unpacking security policy compliance: The motivators and barriers of employees' security behaviors. *Symposium on Usable Privacy and Security*, 22-24 July 2015, Ottawa, Canada, 103-122. Available from: https://www.usenix.org/system/files/conference/soups2015/soups15-paper-blythe.pdf [accessed 1 September 2017].

Bolger, N., Davis, A. and Rafaeli, E. (2003) Diary Methods: Capturing Life as it is Lived. *Annual Review of Psychology*, 54, 579-616.

Bossler, A.M. and Holt, T.J. (2009) On-line Activities, Guardianship and Malware Infection: An Examination of Routine Activities Theory. *International Journal of Cyber Criminology*, 3, 400-420.

Brenner (2004) Toward a Criminal Law for Cyberspace: Distributed Security. *Boston University Journal of Science & Technology Law*, 10(2), 1-105.

Brown, W. (2006) American Nightmare: Neoliberalism, Neoconservatism and De-Democratization. *Political Theory*, 34(6), 690-714.

Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2010) Information security policy compliance: An empiricial study of rationality-based beliefs and information security awareness. *MIS Quarterly*, 34(3), 523-548.

Busch, M., Patil, S., Regal. G., Hochleitner, C. and Tscheligi, M. (2016) Persuasive Information Security: Techniques to Help Employees Protect Organizational Information Security. In Meschtscherjakov *et al.* (eds.) *PERSUASIVE 2016*, LNCS 9638. Zurich: Springer, 339-351.

Cabinet Office (2011) *The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world*. Available from: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf [accessed 1 September 2017].

Cabinet Office (2014) *The UK Cyber Security Strategy Report on Progress and Forward Plans: December 2014.* HMSO. Available from: https://www.gov.uk/government/publications/national-cyber-security-strategy-2014-progress-and-forward-plans [accessed 1 September 2017].

Cabinet Office (2014a) *Cyber security is essential in today's marketplace*. Press Release, 5th November. Available from: https://www.gov.uk/government/news/cyber-security-is-essential-in-todays-marketplace [accessed 1 September 2017].

Cabinet Office (2015) *Cyber insurance joint statement*, 5 November 2015. HMSO. Available from: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/371036/Cyber_Insurance_Joint_Statement_5_November_2014.pdf [accessed 1 September 2017].

Cabinet Office (2015a) *UK Cyber Security: The role of insurance in managing and mitigating risk*. HMSO. Available from: https://www.gov.uk/government/publications/uk-cyber-security-the-role-of-insurance [accessed 1 September 2017].

Cabinet Office (2015b) *Cyber security insurance: New steps to make UK world centre*. Press Release, 23 March 2015. Available from: https://www.gov.uk/government/news/cyber-security-insurance-new-steps-to-make-uk-world-centre [accessed 1 September 2017].

Cabinet Office (2015c) *10 Steps to Cyber Security: Executive Companion*. HMSO. Available from: https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility/10-steps-executive-companion [accessed 1 September 2017].

Cabinet Office (2016) Expanding the Cyber First programme. Speech by Matthew Hancock MP, Minister for Cabinet Office, The Institute of Directors, London, 3 March 2016. Available from: https://www.gov.uk/government/speeches/expanding-the-cyber-first-programme-speech-by-matt-hancock [accessed 1 September 2017].

Cabinet Office (2016a) Keeping Britain safe from cyber attacks. Speech by Matthew Hancock MP, Minister for Cabinet Office, London, 25 May 2016. Available from: https://www.gov.uk/government/speeches/keeping-britain-safe-from-cyber-attacks-matt-hancock-speech [accessed 1 September 2017].

Cabinet Office (2016b) Procurement Policy Note – *Cyber Essentials* Scheme. Action Note 09/14, 25 May 2016. Available from: https://www.gov.uk/government/publications/procurement-policy-note-0914-cyber-essentials-scheme-certification [accessed 1 September 2017].

Caldwell, T. (2016) Making security training awareness training work. *Computer Fraud & Security*, June, 8-14.

Castel, R. (1991) From dangerousness to risk. In Burchell, G., Gordon, C. and Miller, P. (eds.) *The Foucault Effect: Studies in Governmentality*. London: Harvester Wheatsheaf.

CERT (2016) *Common Sense Guide to Mitigating Insider Threats*, 5th Edition. CERT Division, Software Engineering Institute, Carnegie Mellon University. Available from: http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=484738 [accessed 1 September 2017].

Chang, J., Venkatasubramanian, K., West, A. and Lee, I. (2013) Analyzing and Defending Against Web-Based Malware. *ACM Computing Surveys*, 45(4), Article 49.

Charity Commission (2016) Making Digital Work: 12 questions for Trustees to consider. Available from https://www.gov.uk/government/publications/making-digital-work-12-questions-for-trustees-to-consider [accessed 1 September 2017].

Choi, K.C. (2008) Computer Crime Victimisation and Integrated Theory: An Empirical Assessment. *International Journal of Cyber Criminology*, 2, 308-333.

Christie, N. (1986) The Ideal Victim. In Fattah, E.A. (ed.) *From Crime Policy to Victim Policy: Reorienting the Justice System*. Basingstoke: Macmillan.

Clarke, R.V.C. (1983) Situational Crime Prevention: Its Theoretical Basis and Practical Scope. *Crime and Justice*, 4, 225-256.

Clarke, J. and Newman, J. (1997) *The Managerial State*. London: Sage.

Cohen, L. and Felson, M. (1979) Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review*, 44(1), 588-608.

Collins, H.M. (2001) What is tacit knowledge? In Schatzki, E., Knorr Cetina, K. and Von Savigny, E. (eds.) *The Practice Turn In Contemporary Theory*. London: Routledge, 107-119.

Collinson, P. (2016) Online fraud victims should be better protected, not blamed. *The Guardian*, 31 May. Available from: http://www.theguardian.com/money/2016/may/31/online-victims-should-be-better-protected-not-blamed [accessed 1 September 2017].

Collinson, P. (2016a) Banks need to tackle web fraud. *The Guardian*, 30 July 2016. Available from: https://www.theguardian.com/money/2016/jul/30/online-fraud-crime-theft-bank-account [accessed 1 September 2017].

Cone, B.D., Irvine, C.E., Thompson, M.F. and Nguyen, T.D. (2007) A video game for cyber security awareness. *Computers & Security*, 26(1), 63-72.

Corti, L. (1993) Using diaries in social research. *Social Research Update*, 2. Available from: http://sru.soc.surrey.ac.uk/SRU2.html [accessed 1 September 2017].

Crawford, A., and Evans, K. (2012) Crime Prevention and Community Safety. In Maguire, M., and Morgan, R. (eds.) *The Oxford Handbook of Criminology*, 5th ed. Oxford: Oxford University Press, 769-805.

Cross, C. (2013) "Nobody's holding a gun to your head…": Examining current discourses surrounding victims of online fraud. In Richards, Kelly, Tauri and Jaun (eds.) *Crime, Justice and Social Democracy: Proceedings of the 2nd International Conference*, Crime and Justice Research Centre, Queensland University of Technology, Brisbane, QLD, 25-32.

Dang-Pham, D. and Pittayachawan, S. (2015) Comparing intention to avoid malware across contetxs in a BYOD-enabled Australian University: A Protection Motivation Theory approach. *Computers & Security*, 48, 281-297.

D'Arcy, J., Herath, T. and Shoss, M.K. (2014) Understanding employee responses to stressful information security requirements: A coping perspective. *Journal of Management Information Systems*, 31(2), 285-318.

Department for Business, Innovation & Skills (DBIS) (2014) *Cyber Essentials Scheme: Requirements for basic protection from cyber attacks*. HMSO. Available from: https://www.gov.uk/government/publications/cyber-essentials-scheme-overview [accessed 1 September 2017].

Department for Business, Innovation & Skills (DBIS) (2014a) *2014 Information Security Breaches Survey*. HMSO. Available from: https://www.gov.uk/government/publications/information-security-breaches-survey-2014 [accessed 1 September 2017].

Department for Business, Innovation & Skills (DBIS) (2014b) *Cyber Essentials Scheme: Summary*. HMSO. Available from: https://www.gov.uk/government/publications/cyber-essentials-scheme-overview [accessed 1 September 2017].

Department for Business, Innovation & Skills (DBIS) (2015) *Small businesses: What you need to know about cyber security*. HMSO. Available from: https://www.gov.uk/government/publications/cyber-security-what-small-businesses-need-to-know [accessed 1 September 2017].

Department for Business, Innovation & Skills (DBIS) (2015a) *2015 Information Security Breaches Survey*. HMSO. Available from: https://www.gov.uk/government/publications/information-security-breaches-survey-2015 [accessed 1 September 2017].

Department for Business, Innovation and Skills (DBIS) (2015b) *Business Population Estimates for the UK and Regions 2015*. Statistical Release, 14 October 2015. Available from: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/467443/bpe_2015_statistical_release.pdf [accessed 1 September 2017].

Department for Business, Innovation and Skills (DBIS) (2015c) *Digital Economy Strategy 2015-2018*, February 2015. Available from: https://www.gov.uk/government/publications/digital-economy-strategy-2015-2018 [accessed 1 September 2017].

Department for Business, Innovation and Skills (DBIS) (2015d) *Cyber security boost for UK firms*, 16 January 2015. Available from: https://www.gov.uk/government/news/cyber-security-boost-for-uk-firms [accessed 1 September 2017].

Department for Culture, Media and Sport (DCMS) (2015) *UK businesses urged to protect themselves from growing cyber threat*. Press Release, 22 September 2015. Available from: https://www.gov.uk/government/news/uk-businesses-urged-to-protect-themselves-from-growing-cyber-threat [accessed 1 September 2017].

Department for Culture, Media and Sport (DCMS) (2015a) Digital Economy Minister (ED Vaisey MP): *Speech on the Government's work with UK businesses on cyber security*. Internet Security Summit, London, 18 November 2015. Available from: https://www.gov.uk/government/speeches/digital-economy-ministers-speech-on-cyber-security-for-uk-businesses [accessed 1 September 2017].

Department for Culture, Media and Sport (DCMS) (2016) Minister for Digital and Culture Minister (Matthew Hancock MP): *Speech addressing the CBI*. 2nd Annual CBI Cyber Security Conference, London, 14 September 2016. Available from: https://www.gov.uk/government/speeches/minister-for-digital-and-culture-addresses-cbi-conference [accessed 1 September 2017].

Department for Culture, Media and Sport (DCMS) (2016a) Minister for Data Protection (Baroness Neville-Rolfe): *Speech on the EU Data Protection Package: The UK Government's perspective*, Cambridge, 4 July 2016. Available from: https://www.gov.uk/government/speeches/the-eu-data-protection-package-the-uk-governments-perspective [accessed 1 September 2017].

Department for Culture, Media and Sport (DCMS) (2017a) *Cyber Security Breaches Survey 2017*, Main Report, April 2017. Available from: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2017 [accessed 1 September 2017].

Department for Culture, Media and Sport (DCMS) (2017b) Press Release accompanying the *Cyber Security Breaches Survey 2017*, 19 April 2017. Available from: https://www.gov.uk/government/news/almost-half-of-uk-firms-hit-by-cyber-breach-or-attack-in-the-past-year [accessed 1 September 2017].

Department for Digital, Culture, Media and Sport (DCMS) (2017c) Press Release accompanying the Report of the consultation on a new Data Protection Bill, 7 August 2017. Available from: https://www.gov.uk/government/news/government-to-strengthen-uk-data-protection-law [accessed 1 September 2017].

Dhillon, G. and Backhouse, J. (2001) Current directions in security research: Towards socio-organizational perspectives. *Information Systems Journal*, 11(2), 127-153.

Donoghue, J. (2013) Reflection on Risk, Anti-Social Behaviour and Vulnerable/Repeat Victims. *British Journal of Criminology*, 53, 805-823.

Edwards, M. (2016) Assessing the UK's response to threats: Challenges and vulnerabilities. Presentation at the *Westminster e-Forum* Keynote Seminar: Cyber security in the UK: Emerging threats, building resilience and policy priorities. London, 19th May 2016.

Eigenberg, H. and Garland, T. (2008) Victim Blaming. In Moriarty, L.J. (ed.) *Controversies in Victimology*. Newark, NJ: LexisNexis, 21-36.

Elias, R. (1993) *Victims Still*. London: Sage.

Elliott, H. (1997) The use of diaries in sociological research on health experience. *Sociological Research Online*. Available from: http://www.socresonline.org.uk/2/2/7.html [accessed 1 September 2017].

Etzioni, A. (1993) *The Spirit of Community*. New York: Simon Schuster.

European Commission (2013) *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*. Available from: http://ec.europa.eu/digital-agenda/en/cybersecurity [accessed 1 September 2017].

Experian (2013) *Managing Cyber Security as a Business Risk: Cyber Insurance in the Digital Age*. Ponemon Institute Research Report, August 2013. Available from: https://www.experian.com/innovation/thought-leadership/ponemon-study-managing-cyber-security-as-business-risk.jsp [accessed 1 September 2017].

Fattah, E. (1989) Victims and Victimology: The Facts and the Rhetoric. *International Review of Victimology*, 1(1), 43-66.

Fattah, E. (1991) *Understanding Criminal Victimisation*. Ontario: Prentice Hall.

Federation of Small Businesses (2013) *Cyber Security and fraud: The impact on small businesses*. Available from: http://www.fsb.org.uk/docs/default-source/Publications/reports/fsb_cyber_security_and_fraud_paper_final.pdf?sfvrsn=0 [accessed 1 September 2017].

Federation of Small Businesses (2015) *Cyber Security and fraud: The impact on small businesses*, Press Release, 1 September 2015. Available from http://www.fsb.org.uk/media-centre/latest-news/2015/09/24/cyber-security-and-fraud-the-impact-on-small-businesses [accessed 1 September 2017].

Federation of Small Businesses (2016) *UK Small Business Statistics 2016*. Available from: https://www.fsb.org.uk/media-centre/small-business-statistics [accessed 1 September 2017].

Felson, M. (1998) *Crime and Everyday Life*, 2nd ed. Thousand Oaks, CA: Pine Forge Press.

Foucault, M. (1978) Governmentality. In Burchell, G., Gordon, C. and Miller, P. (eds.) (1991) *The Foucault Effect: Studies in Governmentality*. Hemel Hempstead: Harvester Wheatsheaf, 87-114.

Foucault, M. (1982) Afterword: The subject and power. In Dreyfuss, H.L. and Rabinow, P. (eds.) *Michel Foucault: Beyond Structuralism and Hermeneutics*. Chicago: University of Chicago Press.

Fraud Advisory Panel (2016) Victim blaming is not helpful in fight against fraud. Press Release, 24 March 2016. Available at: https://www.fraudadvisorypanel.org/wp-content/uploads/2016/03/Victim-Blaming-is-Not-Helpful-in-Fighting-Fraud-Final-24March16.pdf [accessed 1 September 2017].

Furnell, S. (2012) Routes to security compliance: Be good or be shamed? *Computer Fraud & Security*, 12(1), 12-20.

Furnell, S. and Rajendran, A. (2012) Understanding the influences on Information Security behaviour. *Computer Fraud & Security*, 3, 12-15.

Furnell, S. and Thomson, K. (2009) From culture to disobedience: Recognising the varying user acceptance of IT Security. *Computer Fraud & Security*, February, 5-10.

Furnell, S. and Thomson, K. (2009a) Recognising and addressing "Security Fatigue." *Computer Fraud & Security*, November, 7-11.

Garland, D. (1996) The Limits of the Sovereign State: Strategies of Crime Control in Contemporary Society. *British Journal of Criminology*, 36(4), 445-471.

Garland, D. (1997) Governmentality and the Problem of Crime: Foucault, Criminology, Sociology. *Theoretical Criminology*, 1(2), 173-214.

Garland, D. (2001) *The Culture of Control: Crime and Social Order in Contemporary Society*. Oxford: Oxford University Press.

GCHQ (2013) *Countering the cyber threat to business* (including the *10 Steps to Cyber Security*). In Institute of Directors, *Big Picture*. Available from: https://www.gchq.gov.uk/sites/default/files/directors_IoD_article.pdf [accessed 1 September 2017].

Giddens, A. (1990) *The Consequences of Modernity*. Cambridge: Polity.

Giddens, A. (1991) *Modernity and Self-Identity: Self and Society in the Late Modern Age*. Cambridge: Polity.

Gleason, M.E.J., Bolger, N. and Shrout, P. (2001) *The effects of research design on reports of mood: Comparing daily diary, panel, and cross-sectional designs*. Presented at the Society for Personality and Social Psychology Conference, San Antonio, Texas.

Grabosky, P. (2001) Virtual criminality: Old wine in new bottles? *Social & Legal Studies*, 10, 243-249.

Grierson, J. (2016) Met chief suggests banks should not refund online fraud victims. *The Guardian*, 24 March. Available from: http://www.theguardian.com/uk-news/2016/mar/24/dont-refund-online-victims-met-chief-tells-banks [accessed 1 September 2017].

Gottfredson, M. (1981) On the Etiology of Criminal Victimisation. *The Journal of Criminal Law & Criminology*, 72(2), 714-726.

Grossberg, L. (2005) *Caught in a Crossfire: Kids, Politics and America's Future*. Boulder, CO: Paradigm.

Hall, R. (2004) "It can happen to you": Rape prevention in the age of risk management. *Hypatia*, 19, 1-19.

Harber, K.D., Podolski, P. and Williams, C.H. (2015) Emotional Disclosure and Victim Blaming. *Emotion*, 15(5), 603-614.

Hatherly, D., Leung, D. and MacKenzie, D. (2005) The Finitist Accountant: Classifications, Rules and the Construction of Profits. School of Social & Political Studies, University of Edinburgh. Available from: http://www.sociology.ed.ac.uk/__data/assets/pdf_file/0011/3422/The_Finitist_Accountant.pdf [accessed 1 September 2017].

Hayes, S.C. and Cavior, N. (1980) Multiple tracking and the reactivity of self-monitoring: Positive behaviors. *Behavior Therapy*, 11, 283-296.

Herath, T. and Rao, H.R. (2009) Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, 47, 154-165.

Herath, T. and Rao, H.R. (2009a) Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems*, 18, 106-125.

Herley, C. (2009) So Long, And No Thanks for the Externalities: The Rational Rejection of Security Advice by Users. In *Proceedings of the 2009 New Security Paradigms Workshop*. New York: ACM Press.

Heyward-Mills, D. and De Fonseka, J. (2016) Brexit: What Does it Mean for Data Protection? *Computers & Law*, August/September, 3-4.

Hindelang, M., Gottfredson, M. and Garofalo, J. (1978) *Victims of Personal Crime: An Empirical Foundation for a Theory of Personal Victimisation*. Cambridge, MA: Ballinger.

HM Government (2010) *A Strong Britain in an Age of Uncertainty: The National Security Strategy*. Available from: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-security-strategy.pdf [accessed 1 September 2017].

HM Government (2015) *National Security Strategy and Strategic Defence and Security Review*: *A Secure and Prosperous United Kingdom*. Available from: https://www.gov.uk/government/publications/national-security-strategy-and-strategic-defence-and-security-review-2015 [accessed 1 September 2017].

HM Government (2016) *Cyber Security Breaches Survey 2016*. Available from: https://www.gov.uk/government/publications/cyber-security-breaches-survey-2016 [accessed 1 September 2017].

HM Government (2016a) *Cyber Streetwise launches #quickupdates campaign*. Cyber Street Blog, 26 July 2016. Available from: https://www.cyberstreetwise.com/blog/cyber-streetwise-launches-quickupdates-campaign [accessed 1 September 2017].

HM Government (2016b) *National Cyber Security Strategy 2016-2021*. Available from: https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021 [accessed 1 September 2017].

HM Government (2016c) *Cyber Security Regulation and Incentives Review*. Available from: https://www.gov.uk/government/publications/cyber-security-regulation-and-incentives-review [accessed 1 September 2017].

HM Government (2016d) *National Security Strategy and Strategic Defence and Security Review 2015: First Annual* Report. Available from: https://www.gov.uk/government/publications/national-security-strategy-and-strategic-defence-and-security-review-2015-annual-report-2016 [accessed 1 September 2017].

HM Government (2017) *Cyber Security Breaches Survey 2017*. Available from: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2017 [accessed 1 September 2017].

HM Treasury (2015) *Chancellor's speech to GCHQ on cyber security* (as part of the Spending Review and Autumn Statement 2015), 17 November 2015. Available from: https://www.gov.uk/government/speeches/chancellors-speech-to-gchq-on-cyber-security [accessed 1 September 2017].

Holt, T.J. and Bossler, A.M. (2009) Examining the applicability of lifestyle-routine activities theory for cybercrime victimisation. *Deviant Behavior*, 30, 1-25.

Holt, T.J. and Bossler, A.M. (2013) Examining the relationship between routine activities and malware infection indicators. *Journal of Contemporary Criminal Justice*, 29, 420-436.

Holt, T.J. and Bossler, A.M. (2014) An Assessment of the Current State of Cybercrime Scholarship. *Deviant Behavior*, 35, 20-40.

Holt, T.J. and Bossler, A.M. (2016) *Cybercrime In Progress: Theory and Prevention of Technology-Enabled Offenses*. Abingdon, Oxon: Routledge.

Holt, T.J. and Copes, H. (2010) Transferring subcultural knowledge online: Practices and beliefs of persistent digital pirates. *Deviant Behavior*, 31, 625-654.

Holt, T.J. and Turner, M.G. (2012) Examining Risks and Protective Factors of On-Line Identity Theft. *Deviant Behavior*, 33, 308-323.

Holyst, B. (1982) Scope, Tasks and Aim of Penal Victimology. In Schneider, H.J. (ed.) *The Victim in International Perspective*. New York: DeGruyter.

Home Office (2003) *Respect and Responsibility – Taking a Stand Against Anti-Social Behaviour*. London: Home Office.

Home Office (2013) *Cyber Crime: A review of the evidence*. Home Office Research Report 75. HMSO. Available from: https://www.gov.uk/government/publications/cyber-crime-a-review-of-the-evidence [accessed 1 September 2017].

Home Office (2014) *Cyber Streetwise* (renamed *Cyber Aware* in October 2016). Available from: https://www.cyberaware.gov.uk/ [accessed 1 September 2017].

Hopkins, M. (2016) Business, victimisation and victimology: Reflections on contemporary patterns of commercial victimisation and the concept of businesses a 'ideal victims.' *International Review of Victimology*, 22(2), 161-178.

House of Commons Culture, Media and Sport Committee (2016) *Cyber Security: Protection of Personal Data Online*. Available from: http://www.parliament.uk/business/committees/committees-a-z/commons-select/culture-media-and-sport-committee/inquiries/parliament-2015/cyber-security-15-16/ [accessed 1 September 2017].

House of Commons Science and Technology Committee (2012) *Malware and cyber crime*. HMSO. Available from: http://www.parliament.uk/business/committees/committees-a-z/commons-select/science-and-technology-committee/inquiries/parliament-2010/malware-and-cyber-crime/ [accessed 1 September 2017].

House of Commons Home Affairs Committee (2013) *Report on E-Crime*. HMSO. Available from: http://www.publications.parliament.uk/pa/cm201314/cmselect/cmhaff/70/70.pdf [accessed 1 September 2017].

House of Lords Science and Technology Committee (2007) *Report on Personal Internet Security*. HMSO. Available from:

http://www.publications.parliament.uk/pa/ld200607/ldselect/ldsctech/165/165i.pdf [accessed 1 September 2017].

Hughes, G. (2007) *The Politics of Crime and Community*. Basingstoke: Palgrave.

Ifinedo, P. (2012) Understanding information systems security policy compliance: An integration of the Theory of Planned Behaviour and the Protection Motivation Theory. *Computers & Security*, 31, 83-95.

Ifinedo, P. (2014) Information systems security policy compliance: An empirical study of the effects of socialisation, influence and cognition. *Information & Management*, 51, 69-79.

Iida, M., Shrout, P.E., Laurenceau, J-P. and Bolger, N. (2012) Using diary methods in psychological research. In Cooper, H. (ed.) *APA Handbook of Research Methods in Psychology, Vol. 1: Foundations, Planning, Measures, and Psychometrics*. Washington, DC: American Psychological Association, 277-305.

Impett, E.A, Strachman, A., Finkel, E.J. and Gable, S.L. (2008) Maintaining sexual desire in intimate relationships: The importance of approach goals. *Journal of Personality and Social Psychology*, 94, 808-823.

Information Commissioner's Office (ICO) (2016) Data Protection Act 1998 Supervisory Powers of the Information Commissioner: Monetary Penalty Notice to *Talk Talk* Telecom Group plc. Available from: https://ico.org.uk/media/action-weve-taken/mpns/1625131/mpn-talk-talk-group-plc.pdf [accessed 1 September 2017].

Information Security Forum (2014) From Promoting Awareness to Embedding Behavors: Secure by choice, not by chance. Available from https://www.securityforum.org/uploads/2015/03/From-Promoting-Awareness-ES-2014_Marketing.pdf [accessed 1 September 2017].

Inglesant, P. and Sasse, M.A. (2010) The True Cost of Unusable Password Policies: Password Use in the Wild. *CHI 2010*, April 2010, Atlanta, Georgia, USA. Available from: https://www.cl.cam.ac.uk/~rja14/shb10/angela2.pdf [accessed 1 September 2017].

Institute of Directors (2016) Business need to 'get real' about cyber security. Press Release for Report, entitled *Cyber Security: Underpinning the Digital Economy*, 3

March 2016. Available from: https://www.iod.com/news-campaigns/news/articles/Businesses-need-to-get-real-about-cyber-security [accessed 1 September 2017].

Jewkes, Y. (2007) Cybercrime: Re-thinking crime control strategies. In Jewkes, Y. (ed.) *Crime Online*. Cullompton: Willan.

Johnston, A.C. and Warkentin, M. (2010) Fear appeals and Information Security behaviors: An empirical study. *Management Information Systems Quarterly*, 34(3), 549-566.

Jones, R. (2016) Is Barclays doing enough to protect its customers? *The Guardian*, 12 March 2016. Available from: https://www.theguardian.com/money/2016/mar/12/barclays-fraud-email-con-trick-pressure-bank [accessed 1 September 2017].

Jones, R. (2016a) Email scam costs couple £25,000 – but no one will help. *The Guardian*, 4 March 2016. Available from: https://www.theguardian.com/money/2016/mar/04/fraud-scam-email-barclays-lloyds [accessed 1 September 2017].

Karmen, A. (1990) *Crime Victims: An Introduction to Victimology*. Pacific Grove, CA: Brooks Cole.

Karyda, E., Kiountouzis, E. and Kokolakis, S. (2005) Information security policies: A contextual perspective. *Computers & Security*, 24(3), 246-260.

Kelly, L. (1988) *Surviving Sexual Violence*. Oxford: Polity.

Kemshall, K. (2006) Social policy and risk. In Mythen, G., and Walklate, S. (eds.) *Beyond the Risk Society: Critical Reflections on Risk and Human Security*. Maidenhead: Open University Press, 43-59.

Kenten, C. (2010) Narrating Oneself: Reflections on the Use of Solicited Diaries with Diary Interviews. *Forum: Qualitative Social Research*, 11(2), Art. 16. Available from: http://www.qualitative-research.net/index.php/fqs/article/view/1314/2989 [accessed 1 September 2017].

Kirlappos, I. and Sasse, M.A. (2014) What usable security really means: Trusting and engaging users. *Human Aspects of Information Security: Second Conference, HAS 2014*, Crete, Greece, 22 June. Available from: http://discovery.ucl.ac.uk/1434890/ [accessed 1 September 2017].

Kotulic, A.G. and Clark, J.G. (2004) Why there aren't more information security research studies. *Information & Management*, 41, 597-607.

Kuhn, T.S. (1970) *The Structure of Scientific Revolution*, 2nd Edition. Chicago: University of Chicago Press.

Kuhn, T.S. (1977) *The Essential Tension: Selected Studies in Scientific Tradition and Change*. Chicago: University of Chicago Press.

Kumaraguru, P., Rhee, Y., Aquisti, A. and Nunge, E. (2007) Protecting people from phishing: The design and evaluation of an embedded training email system. In *Proceedings of the 2007 Conference on Computer Human Interaction (CHI 2007)*. New York: ACM Press, 905-914.

Latour, B. (1986) The powers of association. In Law, J. (ed.) *Power, Action and Belief: A New Sociology of Knowledge?* London: Routledge and Kegan Paul.

Latour, B. (1987) *Science in Action*. Cambridge, MA: Harvard University Press.

Leach, J. (2003) Improving user security behavior. *Computers & Security*, 22(8), 685-695.

Lee, D., Larose, R. and Rifon, N. (2008) Keeping our network safe: A model of online protection behaviour. *Behaviour & Information Technology*, 27(5), 445-454.

Leigh Star, S. (1985) Scientific Work and Uncertainty. *Social Studies of Science*, 15(3), 391-427.

Leukfeldt, E.R. and Yar, M. (2016) Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis. *Deviant Behavior*, 37(3), 263-280.

Lessig, L. (1999) *Code and Other Laws of Cyberspace*. New York: Basic Books.

Lessig, L. (2006) *Code Version 2.0*. New York: Basic Books.

Lewis, D. (1969) *Convention: A Philosophical Study*. Cambridge, MA: Harvard University Press.

Litt, M.D., Cooney, N.L. and Morse, P. (1998) Ecological Momentary Assessment (EMA) with treated alcoholics: Methodological problems and potential solutions. *Health Psychology*, 17, 48-52.

LMRMC (2010) Online Riskiness: Questionnaire Results – Overall. LM Research & Marketing Consultancy, 20 September (Unpublished).

Loader, I. and Sparks, R. (2002) Contemporary Landscapes of Crime, Order, and Control: Governance, Risk, and Globalization. In Maguire, M., Morgan, R. and Reiner, R. (eds.) *The Oxford Handbook Handbook of Criminology*, 3r ed. Oxford: Oxford University Press, 83-111.

Lynch, M. (1992) Extending Wittgenstein: The Pivotal Move from Epistemology to the Sociology of Science. In Pickering, E. (ed.) *Science as Practice and Culture*. Chicago: University of Chicago Press.

MacEwan, N. (2013) A Tricky Situation: Deception in Cyberspace. *Journal of Criminal Law*, 77(5), 417-432.

Maimon, D., Wilson, T., Ren, W. and Berenblum, T. (2015) On the relevance of spatial and temporal dimensions in assessing computer susceptibility to system trespassing incidents. *British Journal of Criminology*, 55, 615-634.

Mangold, L.V. (2012) Using ontologies for adaptive information security training. In IEEE Computer Society (2013) *Proceedings of the Seventh International Conference on Availability, Reliability and Security*, ARES 2012, 522-524.

Manning, P. (2000) Policing New Social Spaces. In Sheptycki, J. (ed.) *Issues in Transnational Policing*. London: Routledge.

Manning, N. and Shaw, I. (eds.) (2000) *New Risks, New Welfare: Signposts for Social Policy*. Oxford: Blackwell.

Marcum, C.D. (2008) Identifying potential factors of adolescent online victimisation for high school seniors. *International Journal of Cyber Criminology*, 2(2), 346-367.

Martinson, R. (1974) What Works? – Questions and Answers about Prison Reform. *The Public Interest*, 35(1), 22-54.

Mason, J. (2002) Qualitative Interviewing: Asking, listening and interpreting. In May, T. (ed.) *Qualitative Research in Action*. London: Sage.

Mawby, R.I. and Walklate, S. (1994) *Critical Victimology*. London: Sage.

May, T. (2011) *Social Research: Issues, Methods and Process*, 4th ed. Maidenhead: McGraw-Hill.

McAlinden, A. (2014) Deconstructing victim and offender identities in discourses on child sexual abuse. *British Journal of Criminology*, 54, 180-198.

McDowell, J. (1984) Wittgenstein on following a rule. *Synthese*, 58, 325-364.

Mendelsohn, B. (1956) A new branch of Bio-psychological science: La victimology. *Revue Internationale de Criminologie et de Police Technique*, No.2.

Miers, D. (1989) Positivist Victimology: A Critique. *International Review of Victimology*, 1(1), 3-22.

Miers, D. (1990) *Compensation for Criminal Injuries*. London: Butterworths.

Milne, L. (2014) Flexible working – a new right to request. *The Telegraph*, 6 June. Available from: http://www.telegraph.co.uk/sponsored/business/national-business-awards/10878070/flexible-working-changes-june.html [accessed 1 September 2017].

Mitchell, W.J. (1995) *City of Bits: Space, Place and the Infobahn*. Cambridge, MA: MIT Press.

Monahan, T. (2009) Identity theft vulnerability: Neoliberal governance through crime construction. *Theoretical Criminology*, 3, 155-176.

Mythen, G. (2007) Cutural Victimology: Are we all victims now? In Walklate, S. (ed.) *Handbook of Victims and Victimology*. Cullompton: Willan Publishing.

National Crime Agency (2015) *A Coordinated Response to Cyber Crime – March 2015.* Available from: http://www.nationalcrimeagency.gov.uk/publications/528-a-coordinated-response-to-cyber-crime-march-2015/file [accessed 1 September 2017].

National Cyber Security Centre (2017) *10 Steps to Cyber Security*. Available from: https://www.ncsc.gov.uk/guidance/10-steps-cyber-security [accessed 1 September 2017].

National Cyber Security Centre (2017a) Speech by Ciaran Martin, the NCSC Chief Executive Officer, to the CBI Conference, 13th September 2017. Available from: http://www.cbi.org.uk/news/full-speech-ciaran-martin-on-the-national-cyber-security-centre/ [accessed 14 September 2017].

Newburn, T. (2013) *Criminology*, 2nd ed. Abingdon, Oxon: Routledge.

Newman, G. and Clarke, R. (2003) *Superhighway Robbery: Preventing E-Commerce Crime*. Cullompton: Willan Press.

Ngo, F.T. and Paternoster, R. (2011) Cybercrime Victimisation: An examination of Individual and Situational level factors. *International Journal of Cyber Criminology*, 5(1), 773-793.

Oakeshott, M. (1975) *On Human Conduct*. Oxford: Oxford University Press.

Office of Cyber Security and Information Assurance (OCSIA) (2016) Policy priorities in the UK and EU. Speech by James Snook, Deputy Director for Business, Crime and Skills, OCSIA, Cabinet Office, at *Westminster e-Forum on Cyber Security*, London, 19 May 2016.

O'Malley, P. (1992) Risk, Power and Crime Prevention. *Economy and Society*, 21(3), 252-275.

O'Malley, P. (1998) Neoliberalism and Risk in Criminology. In Anthony, T. and Cuneen, C. (eds.) *The Critical Criminology Companion*. Federation Press, 55-67.

O'Malley, P. (2004) *Risk, Uncertainty and Government*. London: Glasshouse Press.

O'Malley, P. (2006) Criminology and Risk. In Mythen, G., and Walklate, S. (eds.) *Beyond the Risk Society: Critical Reflections on Risk and Human Security*. Maidenhead: Open University Press, 43-59.

Omand, D. (2010) *Securing the State*. London: Hurst.

Osborne, D. and Gaebler, T. (1992) *Re-Thinking Government*. Harmondsworth: Penguin.

Oxford English Dictionary (OED) (2016) Available from: http://www.oed.com/ [accessed 1 September 2017].

Pahnila, S., Siponen, M. and Mahmood, A. (2007) Employees' Behavior Towards IS Security Policy Compliance. *Proceedings of the 40th Annual Hawaii International Conference on System Sciences*. Available from: https://www.researchgate.net/publication/224686893_Employees'_Behavior_towards_IS_Security_Policy_Compliance [accessed 1 September 2017].

Parent, M. and Cusack, B. (2016) Cybersecurity in 2016: People, Technology, and Processes. *Business Horizons*, 59, 567-569.

Parkin, S., Fielder, A. and Ashby, A. (2016) Pragmatic Security: Modelling It Security Management Responsibilities for SME Archetypes. *Proceedings of the 8th ACM CCS International Workshop on Managing Insider Security Threats (MIST 2016)*. Available from: http://dl.acm.org/citation.cfm?doid=2995959.2995967 [accessed 1 September 2017].

Parsons, K., McCormac, A., Butavicius, M. and Ferguson, L. (2010) Human Factors and Information Security: Individual, Culture and Security Environment. Australian Government, Department of Defence (Command, Control, Communications and Intelligence Division). Available from: http://www.dtic.mil/dtic/tr/fulltext/u2/a535944.pdf [accessed 1 September 2017].

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M. and Jerram, C. (2014) Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). *Computers and Security*, 42, 165-176.

Peachey, K. and Johnston, C. (2017) Identity theft at epidemic levels, warns Cifas. *BBC News*, 23 August. Available from: http://www.bbc.co.uk/news/business-41011464 [accessed 1 September 2017].

Peacock, L. (2014) Flexible working: Are UK employers still stuck in the dark ages? *The Telegraph*, 19 June. Available from: http://www.telegraph.co.uk/women/womens-

business/10909359/Flexible-working-Are-UK-employers-still-stuck-in-the-dark-ages.html [accessed 1 September 2017].

Pease, K. (1994) Crime Prevention. In McGuire, M., Morgan, R. and Reiner, R. (eds.) *The Oxford Handbook of Criminology*. Oxford: Oxford University Press.

Pfleeger, S., Sasse, M.A. and Furnham, A. (2014) From Weakest Link to Security Hero: Transforming Staff Security Behavior. *Homeland Security & Emergency Management*, 11(4), 489-510.

Reed, C. (2012) *Making Laws for Cyberspace*. Oxford: Oxford University Press.

Rees, G. (2011) "Morphology is a witness which doesn't lie": Diagnosis by similarity relation and analogical inference in clinical forensic medicine. *Social Science and Medicine*, 73, 866-872.

Rees, G. and White, D. (2012) Vindictive but vulnerable: Paradoxical representations of women as demonstrated in internet discourse surrounding an anti-rape technology. *Women's Studies International Forum*, 35, 426-431.

Reis, H.T. and Gable, S.L. (2000) Event-sampling and other methods for studying everyday experience. In Reis, H.T. and Judd, M.C. (eds.) *Handbook of Research Methods in Social and Personality Psychology*. New York: Cambridge University Press, 190-222.

Reyns, B.W., Henson, B. and Fisher, B.S. (2011) Being pursued online: Applying cyberlifestyle-routine activities theory to cyberstalking victimisation. *Criminal Justice and Behavior*, 38, 1149-1169.

Rhee, H.-S., Kim, C. and Ryu, Y.U. (2009) Self- efficacy in Information Security: Its influence on end-users' information security practice behavior. *Computers & Security*, 28, 816-826.

Rhodes, R. (1997) *Understanding Governance: Policy Networks, Governance, Reflexivity and Accountability*. Buckingham: Open University Press.

Ritchie, J., Lewis, J., McNaughton Nicholls, C. and Ormston, R. (2014) *Qualitative Research Practice: A Guide for Social Science Students & Researchers*, 2nd ed. London: Sage.

Rock, P. (2007) Theoretical perspectives on victimisation. In Walklate, S. (ed.) *Handbook of Victims and Victimology*. Collumpton: Willan, 37-61.

Romer, H. (2014) Best practices for BYOD security. *Computer Fraud & Security*, 1, 13-15.

Rose, N. and Miller, P. (1992) Political Power Beyond the State: Problematics of Government. *British Journal of Sociology*, 43(2), 173-205.

Safa, N.S. and Maple, C. (2016) Human errors in the information security realm – and how to fix them. *Computer Fraud & Security*, September, 17-20.

Sasse, M.A. and Flechais, I. (2005) Usable Security: Why Do We Need It? How Do We Get It? In Cranor, L.F. and Garfinkel, S. (eds.) *Security and Usability: Designing secure systems that people can use*. Sebastopol, US: O'Reilly Publishing, 13-29.

Schatzki, T.R. (2001) Practice mind-ed orders. In Schatzki, E., Knorr Cetina, K. and Von Savigny, E. (eds.) *The Practice Turn in Contemporary Theory*. London: Routledge, 42-55.

Schneier, B. (2000) *Secrets and Lies*: *Digital security in a networked world*. New Jersey: Wiley and Sons.

Schyfter, P. (2016) Function and Finitism: A Sociology of Knowledge Approach to Proper Technological Function. In Franssen *et al.* (eds.) *Philosophy of Technology after the Empirical Turn*. Zurich: Springer, 305-325.

Seale, C. (2012) (ed.) *Researching Society and Culture*, 2nd ed. London: Sage.

Shanker, S.G. (1987) *Wittgenstein and the Turning-Point in the Philosophy of Mathematics*. Albany, NY: State University of New York Press.

Sharrock, W. (2004) No Case to Answer: A Response to Martin Kusch's 'Rule-Scepticism and the Sociology of Scientific Knowledge.' *Social Studies of Science*, 34(4), 603-614.

Sheble, L. and Wildemuth, B. (2009) Research Diaries. In Wildemuth, B. (ed.) *Applications of social research methods to questions in information and library science*. Santa Barbara, CA: Libraries Unlimited, 211-221.

Silverman, D. (2011) *Interpreting Qualitative Data: Methods for Analysing Talk, Text and Interaction*, 4th ed. London: Sage.

Siponen, M., Mahmood, M.A. and Pahnila, S. (2014) Employees' adherence to Information Security policies: An exploratory field study. *Information & Management*, 51(2), 217-224.

Smyth, V. (2015) Cyber security fortresses built on quicksand. *Network Security*, 8, 5-7.

Spalek, B. (2006) *Crime Victims: Theory, Policy and Practice*. Basingstoke: Palgrave Macmillan.

Sparks, R. (2001) Degrees of Estrangement: The Cultural Theory of Risk and Comparative Penology. *Theoretical Criminology*, 5(2), 159-176.

Sparkes, M. (2014) 'Companies should be forced to admit security breaches'. *The Guardian*, 25 March. Available from: http://www.telegraph.co.uk/technology/internet-security/10721659/Companies-should-be-forced-to-admit-security-breaches.html [accessed 1 September 2017].

Srivastava, A. and Thomson, S.B. (2009) Framework Analysis: A qualitative Methodology for Applied Policy Research. *Journal of Administration & Governance*, 4(2), 72-79.

Stanko, E. (1990) *Everyday Violence: Women's Mad Men's Experience of Personal Danger*. London: Pandora.

Stanton, B., Theofanos, M.F., Prettyman, S.S. and Furman, S. (2016) Security Fatigue. *IT Pro*, September/October 2016, 26-32.

Steves, M., Chisnell, D., Sasse, M.A., Theofanos, M. and Wald, H. (2014) Report: Authentication Diary Study. *National Institute of Standards and Technology*, U.S. Department of Commerce. NISTIR 7983. Available from: http://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7983.pdf [accessed 1 September 2017].

Stone, A.A., Kessler, R.C. and Haythornthwaite, J.A. (1991) Measuring daily events and decisions: Decisions for the researcher. *Journal of Personality*, 59(3), 575-607.

Sturdy, S. (2007) Knowing Cases: Biomedicine in Edinburgh, 1887-1920. *Social Studies of Science*, 37(5), 659-689.

Swaminathan, A., Stone, K. and Schroder, C. (2016) A Shifting Cybersecurity Landscape: Coming Changes and Perils. *Computers & Law,* June/July, 23-25.

Symantec (2015) *Internet Security Threat Report*, Volume 20, April 2015. Available from: https://www.symantec.com/connect/blogs/ncsam-group-article-symantec-2015-internet-security-threat-report-vol-20 [accessed 1 September 2017].

Symantec Corporation (2016) *Internet Security Threat Report*, Volume 21, April 2016. Available from: https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf [accessed 1 September 2017].

Symantec Corporation (2017) *Internet Security Threat Report*, Volume 22, April 2017. Available from: https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf [accessed 1 September 2017].

Szor, P. (2005) *The Art of Computer Virus Research and Defense*. Addison-Wesley.

Taylor, R.W., Caeti, T.J., Loper, D.K., Fritsch, E.J. and Liederbach, J. (2006) *Digital crime and digital terrorism*. Upper Saddle River, NJ: Pearson Prentice Hall.

Tilley, N. and Laycock, G. (2002) *Working Out What To Do: Evidence-based crime reduction*. Crime Reduction Series Paper 11. London: Home Office.

Timmermans, S. and Berg, M. (1997) Standardization in Action: Achieving Local Universality through Medical Protocols. *Social Studies of Science*, 27(2), 273-305.

Travis, A. (2016) Cybercrime figures prompt police call for awareness campaign. *The Guardian*, 21 July 2016. Available from: https://www.theguardian.com/uk-news/2016/jul/21/crime-rate-online-offences-cybercrime-ons-figures [accessed 1 September 2017].

Tunnell, K.D. (1992) *Choosing Crime: The criminal calculus of property offenders*. Chicago: Nelson Hall.

Unsworth, K.L. and Clegg, C.A. (2004) The Study of New Areas Within Employee Innovation Using Diary Methods. Presented at the *18th Annual Australian & New Zealand Academy of Management Conference*, December, Dunedin, New Zealand. Available from: http://eprints.qut.edu.au/3032/ [accessed 1 September 2017].

Valentine, J.A. (2006) Enhancing the employee security awareness. *Computer Fraud & Security*, 6, 17-19.

Vance, A. and Siponen, M. (2012) IS Security Policy Violations: A Rational Choice Perspective. *Journal of Organizational and End User Computing*, 24(1), 21-41.

Vance, A., Siponen, M. and Pahnila, S. (2012) Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. *Information & Management*, 49, 190-198.

Van Dijk, J. (1997) Introducing Victimology. Ninth Symposium of the World Society of Victimology, Amsterdam.

Van Wijk, J. (2013) Who is the 'little old lady' of international crime? Nils Christie's concept of the ideal victim reinterpreted. *International Review of Victimology*, 19(2), 159-179.

Van Wilsem, J. (2011) Worlds tied together? Online and non-domestic routine activities and their impact on digital and traditional threat victimisation. *European Journal of Criminology*, 8, 115-127.

Van Wilsem, J. (2013a) Hacking and Harassment – do they have something in common? Comparing risk factors for online victimisation. *Journal of Contemporary Criminal Justice*, 29, 437-453.

Van Wilsem, J. (2013b) "Bought it, but never got it": Assessing risks factors for online consumer fraud victimisation. *European Sociology Review*, 29, 168-178.

Verizon (2016) *2016 Data Breach Investigations Report*. Available from: http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf [accessed 1 September 2017].

Verizon (2017) *Data Breach Investigations Report*, April 2017. Available from: http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/ [accessed 1 September 2017].

Von Hentig, H. (1948) *The criminal and his victim: Studies in the sociobiology of crime*. Hamden, CT: Archon Books.

Vuchinich, R., Tucker, J. and Harlee, L. (1988) Behavioral assessment. In Donovan, D.M. and Marlatt, G.A. (eds.) *Assessment of addictive behaviors*. New York: Guildford Press, 51-83.

Walklate, S. (1989) *Victimology: The Victim and the Criminal Justice Process*. London: Unwin Hyman.

Walklate, S. (1992) Appreciating the Victim: Conventional, Realist or Critical Victimology? In Young, J. and Matthews, R. (eds.) *Issues in Realist Criminology*. London: Sage, 102-118.

Walklate, S. (1997) Risk and criminal victimisation: A modernist dilemma? *British Journal of Criminology*, 37(1), 35-45.

Walklate, S. (2011) Reframing criminal victimisation: Finding a place for vulnerability and resilience. *Theoretical Criminology*, 15, 179-194.

Wall, D.S. (2013) Enemies within: Redefining the insider threat in organizational security policy. *Security Journal*, 26(2), 107-124.

Ward, M. and Rhodes, C. (2014) Small businesses and the UK economy. Standard Note: SN/EP/6078. House of Commons Library. Available from: http://researchbriefings.parliament.uk/ResearchBriefing/Summary/SN06078 [accessed 1 September 2017].

Webb, B. and Webb, S. (1932) *Methods of Social Study*. London: Longmans Green.

Wheeler, L. and Reis, H.T. (1991) Self-recording of everyday life events: Origins, types, and uses. *Journal of Personality*, 59(3), 339-354.

Whitehouse, O. (2016) Latest developments in protecting key industries: Common issues and sector-specific challenges. Presentation at the *Westminster e-Forum* Keynote Seminar: Cyber security in the UK: Emerging threats, building resilience and policy priorities. London, 19th May 2016.

Whitson, J.R. and Haggerty, K.D. (2008) Identity theft and the care of the virtual self. *Economy and Society*, 37(4), 572-594.

Wickstrom, G. and Bendix, T. (2000) The "Hawthorne Effect" – what did the original Hawthorne studies actually show? *Scandinavian Journal of Work, Environment & Health*, 26(4), 363-367.

Wildavsky, A. (1988) *Searching for Safety*. Oxford: Transition.

Wilson, J.Q. (1975) *Thinking About Crime*. New York: Vintage.

Wilson, M. and Hash, J. (2003) Building an information technology security awareness and training program. National Institute of Standards and Technology. Available from: https://www.nist.gov/publications/building-information-technology-security-awareness-and-training-program [accessed 1 September 2017].

Wittgenstein, L. (1967) *Philosophical Investigations*. Oxford: Blackwell.

Wittgenstein, L. (1967a) *Zettel*. Oxford: Blackwell.

Wittgenstein, L. (1969) *On Certainty*. Oxford: Blackwell.

Wittgenstein, L. (1978) *Remarks on the Foundations of Mathematics*. Oxford: Blackwell.

Wolfgang, M. (1958) *Patterns in Criminal Homicide*. New York: New York University Press.

Wood, J. and Shearing, C. (2006) Security and nodal governance. Prepared for seminar at the Temple University Beasley School of Law, Philadelphia, 25 October 2006. Available from: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.574.2442&rep=rep1&type=pdf [accessed 1 September 2017].

Woolfe, S.E, Higgins, G.E. and Marcum, CD. (2008) Deterrence and digital piracy: A preliminary examination of the role of viruses. *Social Science Computer Review*, 26, 317-333.

World Economic Forum (2014) *Insight Report: Global Risks*, 9th Edition. Available from: http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2014.pdf [accessed 1 September 2017].

Yar, M. (2005) The novelty of 'cybercrime': An assessment in light of routine activity theory. *European Journal of Criminology*, 2, 407-427.

Young, J. (1992) Ten points of realism. In Young, J. and Matthews, R. (eds.) *Rethinking Criminology: The Realist Debate*. London: Sage, 24-68.