Using Psychological Theories and Usable Security to Understand Cyber-Security Perceptions and Behaviours Within an Organisation; a Case Study of a Law Firm.

Georgia Crossland

Using Psychological Theories and Usable Security to Understand Cyber-Security Perceptions and Behaviours Within an Organisation; a Case Study of a Law Firm.

Georgia Crossland

Thesis submitted to Royal Holloway, University of London in fulfilment of the degree of Doctor of Philosophy in Information Security.

Centre For Doctoral Training in Cyber Security,
Information Security Group,
Royal Holloway, University of London

Supervisor: Dr Rikke Bjerg Jensen

May 2022

Declaration of Authorship

I, Georgia Crossland, declare that this work was carried out in accordance with the Regulations of the University of London. I declare that this submission is my own work, and to the best of my knowledge does not represent the works of others, published or unpublished, except where duly acknowledged in the text. No part of this thesis has been submitted for a higher degree at another university or institution.

Signed: Georgia Clare Crossland Date: 25/05/2022

Acknowledgements

Firstly, thank you to my supervisor, Dr Rikke Bjerg Jensen, for your continued support and encouragement throughout the PhD process. Your guidance helped me bridge the gap between psychology and information security, making my thesis what it is today.

Thank you to the EPSRC and the Centre for Doctoral Training (CDT) in Cyber Security, Royal Holloway for the opportunities the PhD has allowed me. This programme not only enabled me to grow as a researcher, but to explore my interests outside academia.

A big thank you must also go to Drs (or soon to be) Laura Shipp, Amy Ertan, Aoiffe Walsh and Liam Fitzgerald, for their unwavering friendship and support through this five year(!) process. Their constant encouragement (both academic and otherwise) gave me the ability to see the PhD to the end. An extra thanks to Amy and Laura, for all the cyber security related adventures outside the PhD.

Many many thanks to my mum, sister and dad, as well as Manuela Sanchiz Garin for supporting me in countless ways throughout my BSc, MSc and now PhD.

Abstract

Cyber-security practice is dominated by a focus on attempting to remove “the human” from cyber-security processes, with industry often creating policies that constrain and monitor individuals. Moreover, most existing cyber-security research employs quantitative methods of inquiry and analysis, which has resulted in a lack of qualitative cyber-security research within organisations. Positioned in usable security scholarship, this thesis uses psychological theories (PMT, the EPPM and the TPB) to explore cyber-security culture, perceptions, biases and behaviour within the context of a single organisation. This research presents and reports on a case study of a global law firm. Interviews and focus groups were conducted with 40 participants, who were all employees of this firm. Research findings emerged through an interpretative thematic analysis of focus group and interview data. Through this analysis, four distinct themes were constructed and, hence, form the core of the present thesis. More specifically, these themes comprised (1) organisational perceptions of security culture, (2) the individual human element, (3) perceptions of cyber security training and policies, and (4) the COVID-19 pandemic and the move to remote working. Throughout this work, these themes are put into conversation with psychological theories, heuristics and biases, alongside usable security scholarship, to deepen interpretation and understanding of research findings. By discussing these findings with relevance to psychological theories and usable security, this thesis demonstrates the benefits of positioning the research within these domains to understand cyber-security perceptions and behaviours in a qualitative research context. This thesis shows how academia and industry can work together to conduct human-focused cyber-security research within organisations. The theoretical, methodological and empirical contributions of these findings are discussed, together with suggestions for future research.

Publications

Some of the material of this thesis contributed to other previously published work. Part of the literature review contributed to a report for the Cabinet Office: *Cyber Security Behaviour in Organisations* (Ertan, Crossland, Heath, Denny & Jensen, 2020). Some writing from the literature review also contributed to a report for the Research Institute for Sociotechnical Cyber Security (RISCS): *Remote Working and (In)Security* (Crossland & Ertan, 2021). Chapters from this thesis are also being submitted to conferences and journals for publication.

Table of Contents

List of Tables

List of Figures

Chapter 1. Introduction

1.1 Research Introduction

Human factors in cyber security are of great importance to organisations, as demonstrated by an abundance of research (Da Silva & Jensen, 2022; Sabillon, 2022; Uchendu et al., 2021; von Solms & von Solms, 2018). Government reports suggest that in 2020, 46% of businesses and 26% of charities suffered a security breach in the previous 12 months (Cyber Security Breaches Survey, 2020). Among large businesses, the percentage of security breaches was higher still, at 75%. Most of the breaches were reported to have entered organisations via staff, for example, through phishing emails (Cyber Security Breaches Survey, 2020). In addition to issues directly caused by such cyber-attacks and hacks, such as monetary loss, research has found that the organisational harm caused by cyber-attacks propagates, causing physical and digital harm; economic harm; psychological harm; reputational harm; and social and societal harm (Agrafiotis et al., 2018). These statistics and the surrounding research imply that further study is still needed to understand the reasons for human-centred breaches in cyber security. In the last few decades, there has been a growing body of research looking to investigate the role of the human factor within cyber-security systems. Such research draws from multi-disciplinary areas rooted in behavioural science.

Research on human factors in cyber security continues to be dominated by a focus on attempting to remove the human element from the cyber security process (Whitman, 2003; Zimmermann & Renaud, 2019). This is perhaps partly due to the number of security breaches believed to stem from the human factor, with research showing that cyber security concerns usually include human actors (Zimmermann & Renaud, 2019). However, this focus on removing, controlling, and monitoring the human factor remains despite a growing interest in foregrounding positive human and social factors within cyber security, particularly in the context of usable security (Crossler et al., 2013; Furnell et al., 2007; Inglesant & Sasse, 2010; Sasse & Flechais, 2005). Understanding perceptions, biases, security culture, and security behaviours within organisations to improve cyber security remains under-researched, especially the research of these factors holistically. At the same time, technology has become

ever more present within organisations and in people's professional lives, making individuals and organisations more vulnerable to cyber-security threats, with the range of threats rapidly increasing (Tsakalidis et al., 2018; Van Schaik et al., 2018). The lack of research on human factors combined with increasing security threats demonstrates the importance of studying human factors in cyber security positively, as constraining and controlling the human factor continues to be proven disadvantageous. For example, the methods used to control and monitor humans in cyber security, such as phishing simulations and monitoring tools, have been criticised for their ethics and efficaciousness (Kirlappos & Sasse, 2011; Kumaraguru et al., 2010).

The 'user' and other human factors of cyber security within organisations have been researched since Jerome Saltzer and Michael Schroeder published their foundational paper in 1975. This paper highlighted ten principles for designing security, three of which relied heavily on the human factor and behavioural sciences (Saltzer & Schroeder, 1975). These behavioural principles are as follows; Psychology: the security mechanism must be 'psychologically acceptable' to the humans who must use it; Human Factors and Economics: each individual user, and the organisation as a whole, should have to deal with as few distinct security mechanisms as possible; Crime Science and Economics: the effort required to beat a security measure should exceed the resources and potential rewards for the attacker. However, it is arguably not until the last few decades that user-centred research in cyber security has picked up a significant pace. Previously, much research, as will be discussed in Chapter 2 of this thesis, ignored the idea put forward by Saltzer and Schroeder (1975) that security measures, technologies and policies need to be usable and acceptable to be effective. More recently, the user has begun to be viewed as part of the solution to cyber security (Sasse et al., 2001) rather than cyber security's biggest weakness, which is still a prevailing view in some research (Goo et al., 2014; Hughes-Lartey et al., 2021; Lowry & Moody, 2015; Sabillon, 2022).

Psychological scholarship has been applied to cyber security to aid understanding of why individuals may behave in what security professionals see as a non-compliant manner. Behavioural theories such as Protection Motivation Theory (Prentice-Dunn & Rogers, 1986), the Extended Parallel Process Models (Witte, 1996) and the Theory of Planned Behaviour

(Ajzen, 1985) have been applied to this area (Blythe et al., 2015; Bulgurcu et al., 2010; Chen et al. 2021; Haag et al., 2021; Herath & Rao, 2009b; Masuch et al., 2021; Sommestad, 2015). Such theories attempt to understand how individuals behaviourally respond to risk or the antecedents to changing behaviour. Early psychological theory and research on heuristics and biases have also been applied to the area of cyber security, demonstrating how humans' natural inclinations regarding risk might impact their risk perception (Campbell et al., 2007; Chmielarz & Szumski, 2019; Cho et al., 2010; Haltinner et al., 2015; Kim et al., 2018). However, the use of psychology in this area has often been to help increase compliance and help change behaviour without looking at the problems and experiences of employees. Much of this research has focused on implementing cyber-security training and awareness campaigns within organisations to influence and change human behaviour. Moreover, such studies have predominantly been survey- or questionnaire-based, testing the concepts and their relative impact on the intention of employees to inform behaviours (Iuga et al., 2016; Flores et al., 2014; Kirlappos & Sasse, 2011; Renaud, 2011; Sheng et al., 2010; Vance et al., 2012). Researchers have called for more qualitative research, as well as research where academia and industry work together (Uchendu et al., 2020).

Psychological and other human-factors based research in cyber security has largely been rooted within organisational contexts and has been driven by a few behavioural disciplines. Research in this area has looked at the internal and individual factors that drive and influence human behaviour. For example, within organisations, how internal biases might affect behaviour (Tsohou et al., 2015), the emotional experiences of cyber-attacks (Bada & Nurse, 2020; Budimir et al., 2021), or the influencing factors of cyber-security culture (Halevi et al., 2016; Uchendu et al., 2021). Psychology has also been a big influence on cyber-security training and awareness campaigns, where theories of perceptions of risk and behaviour change have been applied to the area of employee compliance in cyber security (Herath & Rao, 2009b; Sommestad et al., 2015). However, some of this research has been criticised by other psychological researchers in the area and by another fraction of cyber-security research, namely usable security, for certain methods, such as the use of fear appeals and other persuasion techniques shown to be unsuitable (Bada et al., 2019). These criticisms question the ethics of scaring individuals into 'behaving' as well as query the efficaciousness of fear appeals (Bada et al., 2019).

The field of usable security, the seminal papers of which used psychological principles (Weirich & Sasse; 2001; Norman, 1988), argues that the strength of security is determined by the degree to which security is usable (Adams & Sasse, 1999; Beautement & Sasse, 2009; Inglesant & Sasse, 2010; Nurse et al., 2011b; Weirich & Sasse; 2001; Zurko & Simon, 1996). This field is where scholars, such as Adams and Sasse (1999), identified users to be part of the solution rather than the problem in cyber security. Before this field emerged as an established body of research, cyber security and usability have often been regarded as competing system goals (Nurse et al., 2011a). However, research now shows cyber security to necessitate usability (Adams & Sasse, 1999; Sasse et al., 2001). It is further argued that when security measures and policies have failed previously, it is because they were not usable or workable, not because the human is an inherent 'weakness' in cyber-security processes. This discipline can be exemplified by one of its earliest pieces of literature by Sasse et al. (2001), where it was demonstrated that password policies and mechanisms agreed upon by security experts were routinely bypassed by employees and therefore did not work at all in practice. Since the seminal paper by Adams and Sasse (1999), the field has gone through several significant stages, or 'waves' (Bødker, 2006). The usable security field went from looking solely at the individual to researching a broader range of social behaviours and, even more recently, understanding the integration of technology into people's everyday lives (Coles-Kemp & Hansen, 2017).

Despite such research, the perspective of the human as the problem or 'weak link' in cyber security is still often the mainstream view (Goo et al., 2014; Hughes-Lartey et al., 2021; Lowry & Moody, 2015; Sabillon, 2022). However, there is a sense that this might be changing (Zimmermann & Renaud, 2019). Based on this, researchers argue that human-centred security and privacy research still lacks maturity in many ways (Renaud & Flowerday, 2017). Furthermore, psychological theory and usable security are rarely looked at together to provide deep insight into human behaviour of cyber security within qualitative work inside organisations.

1.2 A Note on Defining Cyber Security

It is clear from academic articles, security-related conference proceedings and many other pieces of literature that cyber security is a topic of great attention and considerable interest to a broad spectrum of stakeholders. However, what is less clear is the definition of cyber security and why it is often used interchangeably with the term information security within media and research (Reid & Van Niekerk, 2014; von Solms & van Niekerk, 2013; von Solms & von Solms, 2018). The terms themselves are contested within research and do not have one singular definition or meaning (von Solms & van Niekerk, 2013). Therefore, as well as investigating cyber security in terms of the interplay between how individuals and organisations may reduce the risk of cyber-attack, researchers have also sought to understand and define cyber security and information security and describe their similarities and differences. This is an essential venture as it would be hard to convince organisations and employees that cyber security is important and partly their responsibility without being able to give a comprehensive definition or explanation of the concept (von Solms & von Solms, 2018). Moreover, they are crucial terms to define for research, as, despite their interchangeable use within the literature, researchers argue they include different factors (von Solms & van Niekerk, 2013). For research, such as the current, which looks at human factors, this becomes an even more important distinction, as cyber security has been deemed more inclusive of human elements (von Solms & van Niekerk, 2013).

In their 2013 paper, von Solms and van Niekerk argue that, although there is extensive overlap between cyber security and information security, these two terms are not wholly analogous, even if they share certain factors. Moreover, the paper posits that the term cyber security adds additional factors to the traditional term information security. For example, cyber security includes the protection of information resources and other assets, including the human element. In information security, reference to the human factor generally relates only to the role of the human factor in the security process (von Solms & van Niekerk, 2013). Von Solms and van Niekerk argue that cyber security adds to the human factor by including humans as potential targets of cyber-attacks or even unknowingly participating in a cyber-attack. This additional dimension has implications for society since the protection of vulnerable groups is considered and it, therefore, extends the term information security in

this way. Based on this, researchers have argued that the term cyber security is more suitable for human-based research, as this term focusses more heavily on significance to humans (Slupska, 2019).

Other papers attempt to demonstrate the differences between information-security culture and cyber-security culture (Reid & van Niekerk, 2014). These papers argue that information security culture refers to the involvement of human factors to protect information in an organisational context. For example, an information-security culture helps protect a company from a wide range of threats to ensure business continuity, minimise business risk and maximise return on investments. On the other hand, Reid and Van Niekerk argue that cyber-security culture extends information security and involves the protection of the interests of a person, society or nation, including protecting their assets from risks relating to their contact with 'cyberspace'. Both Reid and van Niekerk (2014) and von Solms and van Niekerk (2013) argue, therefore, that cyber security and information security cover much of the same process. They both further suggest that cyber security extends the concept of information security by adding more comprehensive human elements and the protection of such elements to the definition.

Other research further highlights that although cyber security has emerged as a widely used term in the academic literature and by practitioners and politicians, it appears as fashionable jargon and with little understanding of the terms. For example, Schatz et al. (2017) conducted a literature review to identify the main definitions of cyber security, finding 28 sources that matched their criteria. Through analysis of the key components of each definition, Schatz et al. (2017) propose what they refer to as an 'improved' and more representative definition of cyber security; 'the approach and actions associated with security risk management processes followed by organisations and states to protect confidentiality, integrity and availability of data and assets used in cyber space. The concept includes guidelines, policies and collections of safeguards, technologies, tools and training to provide the best protection for the state of the cyber environment and its users' (Schatz et al., 2017, p. 66).

The terms information security and cyber security are explained here to give context to this research space. However, it is necessary to highlight that those participating in the current research would not be exceedingly familiar with the differences between these terms, or perhaps even the terms themselves. Furthermore, information security and cyber security are used interchangeably within the literature, with some research cited in this thesis referring to cyber security and some using information security without apparent conceptual differences.

Despite potential issues with the term, in the current research, the choice was made to use the term cyber security instead of information security for consistency throughout the research and ease of reading. This follows other research in the field, which suggests that when research has a focus on people, the term cyber security is more appropriate (Slupska, 2019), as von Solms and van Niekerk (2013) found this term to include more human concepts.

1.2.1 A Note on Defining 'Human Factor' Terms

It is further necessary to more closely look at terms related to the non-technological aspects of cyber security, given this is the focus of the current research. This section of the thesis will define what is meant by 'human factors in cyber security', 'human aspects of cyber security' and 'usable security'.

This thesis defines 'human factors of cyber security' to include, but does not limit the term, to individual human facets (such as perceptions and biases), social facets (such as cyber-security culture and sub-cultures as well as how people may be managed within their organisations) and societal facets (such as the impact government policy on cyber-security behaviour) (Adams & Sasse, 1999; Slupska, 2019; Solms & van Niekerk, 2013). Human factors and human aspects are used synonymously in the cyber-security literature. This is likely because, per the Oxford Dictionary definition of 'aspect' (Oxford University Press, n.d.), human aspects of cyber security refer to features of human factors of cyber security. For example, biases are an aspect of human factors within cyber security. Human factors and

human aspects of cyber security are terms that appear consistently in many different literatures, studies, dialogues, and theories regarding cyber security (Adams & Sasse, 1999; Nurse et al., 2011a; Renaud & Flowerday, 2017; Sasse et al., 2001). Although they are rarely explicitly defined.

Usable security on the other hand, the term usable security was arguably coined by specific academics in the field of cyber security (Sasse & Flechais, 2005), and is considered to be a branch of scholarship focussing on human-centred security and privacy (Renaud & Flowerday, 2017). This scholarship originally came into being because researchers have pointed out that cyber-security tools, policies and expectations are often simply too complex for many users. The complexity of such cyber-security tools, policies and expectations therefore often result in issues, such as non-compliance, which are readily attributed to users' carelessness and ignorance (Sasse et al., 2001). Usable security scholars therefore aim to create cyber security environments and policies that work for people. The evolution of this scholarship and the research it includes is discussed in-depth in section 2.5 of this thesis.

1.3 Research Aim

The aim of the current research was to provide insight into the cyber-security culture, perceptions, biases, and behaviours of employees in the workplace. This research aim was tackled by two research questions which will be described in the next section of this thesis and will indicate the focus and approach of the current research. For the purpose of the current research, this section will describe the scope of this aim, owing to the overlap between the terms culture, perceptions, biases and behaviours.

The term cyber security culture (discussed in further depth in section 2.7.2) is also referred to as information-security culture and security culture within the literature. In the current thesis the term refers to an omnipresent set of assumptions, norms, and values developed and shared by colleagues of an organisation towards different aspects of cyber security (D'Arcy & Greene, 2014; Ertan et al., 2020). Cyber-security perceptions refer to how cyber security is seen and understood by individuals (Haney & Lutters, 2018), in the current research, this

means by the employees interviewed in the case study. Perceptions may include expressed opinions and beliefs stated by employees during interviews and focus groups, as well as assumptions of others' perceptions. Biases, in the current research, as well as the majority of literature in psychology and cyber security, refers to cognitive biases. Broadly, cognitive bias refers to a systematic (non-random and predictable) departure from rationality in judgment and decision-making (Haselton, Nettle & Andrews, 2015). For example, individuals might base all judgements about the validity of an email on one phishing email they have previously seen. In the current research, the literature review focuses on a few biases that were found to be present in the findings. Behaviours are also included explicitly in the aims as the current research wanted to make sure that participants *actions*, were also understood.

1.4 Research Questions

This research took a case-study approach to gain a deeper understanding of cyber-security behaviours in an organisation through the lens of cognitive and social psychology and usable security. This research adopted a single case-study approach of a global law firm to gain a deep understanding of cyber-security behaviours and perceptions in an organisational context. The case-study approach allows for detailed, multi-faceted investigations of complex issues in real-life settings (Crowe et al., 2011). In-depth interviews and focus groups were used as the methods for data collection. Two separate yet interlinked research questions underpinned this research to inform the research aim. The first question seeks to investigate cyber-security culture, perceptions, biases and behaviours, and the second question seeks to help interpret findings in order to provide deeper insight. These are outlined below.

1) How can cyber-security culture, perceptions, biases and behaviours be understood in the context of a case study within a single organisation, and what are the dynamics between these constructs?

The goal of this question is to qualitatively explore the cyber-security culture, behaviours, perceptions, and biases within the context of a single organisation. This includes perceptions

of cyber-security policies and training. Through this research question, we aimed to understand how cyber-security behaviours and perceptions manifest within a single organisation and how perceptions and behaviours might be linked. The research hopes to shed light on nuances that might be lost when combining data from multiple organisations by looking at a single organisation. Previous research often looks at cyber-security concepts separately, such as security culture, and does not explore different cyber-security factors within an organisation. Moreover, much previous research is based on surveys and questionnaires. In contrast, the current research aims to provide deep qualitative insights into these phenomena.

2) How can psychological theories (PMT, the EPPM and the TPB), along with usable security scholarship, be used to deepen these understandings?

This research question does not aim to test correlations between constructs of the respective theories, or how individual constructs influence and impact behavioural intention or cyber-security behaviour. Rather, here, the current research looks at how, and to what extent, the concepts underpinning these psychological theories, PMT (Prentice-Dunn & Rogers, 1986), the EPPM (Witte, 1996) and the TPB (Ajzen, 1985), apply to cyber-security behaviour and perceptions within organisations using a qualitative case-study methodology. This will be done alongside research relating to usable security. For example, previous research looking at how policy usability might influence employee behaviour will be applied to understand behaviours in the current study. Furthermore, the degree to which such theories and the usable security dialogue can be brought into conversation to explain perceptions and behaviours will be researched.

1.5 Thesis Outline

Chapter 2 of this thesis will discuss the relevant literature that has influenced and paved the way for this research. This literature includes previous studies of cyber security behaviour within organisations, mainly from the fields of psychology, usable security, and more general

human-computer interaction (HCI) research within cyber security. The chapter will then look at previous behaviour theories from psychology, namely Protection Motivation Theory (Prentice-Dunn & Rogers, 1986), the Extended Parallel Process Models (Witte, 1996) and the Theory of Planned Behaviour (Ajzen, 1985), and their application to cyber security. In addition, the chapter will discuss theory and research relating to perceptions and biases that have been found to influence people's cyber-security perceptions and behaviours. The literature review will then look at the usable security dialogue and other related pieces of research. Usable security has been separated from psychology, as although they share foundational knowledge, they are different disciplines. Usable security contains within it many waves of cyber security research, one if which has a more psychological base (Bødker, 2006; Renaud & Flowerday, 2017), but is still not synonymous. Finally, the literature review will demonstrate research on the impact of COVID-19 and remote working on people's cyber-security behaviour within an organisation, given that the current research took place in this period.

Chapter 3 will describe the motivations and details of the methods used in the current research. This chapter will look at the use of case studies, interviews and focus groups, as well as the strengths and weaknesses of these methods. The methodology will also discuss online focus groups and interviews due to circumstances around the COVID-19 pandemic. This methodology chapter will also look at the analysis process, from the automated transcription process to the data analysis using NVivo 12. A discussion of the impacts of the COVID-19 pandemic on this specific research will be detailed, as will an overall reflection of the research journey itself. The last section of the methodology chapter will briefly describe the themes that emerged from the analysis of the data.

The four main themes that emerged from the data, and their respective discussion sections, Chapter 4: organisational perceptions of security culture; Chapter 5: the individual human element; Chapter 6: perceptions of cyber-security training and policies; and Chapter 7: the COVID-19 pandemic and the move to remote working, will then be examined as individual chapters in turn. The findings pertaining to each theme will be described within each chapter before being discussed in relation to existing theory and research; Protection Motivation Theory (Prentice-Dunn & Rogers, 1986), the Extended Parallel Process Models (Witte, 1996)

and the Theory of Planned Behaviour (Ajzen, 1985) as well as previous usable security. Although these sections have clear thematic differences, similarities and overlaps between the main themes and subthemes will be demonstrated.

Finally, the concluding chapter of this thesis will summarise the contributions, limitations and future directions of the current research. The contributions will be theoretical, empirical and methodological and relate to the field of human factors in cyber security as well as how the current organisation and industry might make use of the current findings. Lastly, the conclusion will discuss some limitations of the current research, as well as future directions for human factors in cyber-security research in order to promote positive security and to bridge the research gap between academia and industry.

Chapter 2. Literature Review

2.1 Structure of the Literature Review

This literature review narrows its focus by drawing on theory and research grounded in psychology, such as behaviour change theories and usable security. By drawing on such cyber-security fields, the current literature review looks at how previous research has influenced the study of human factors in cyber-security research within organisations and identifies gaps in the literature. Much of this literature comes from the broader umbrella field of HCI. The current research is organisationally focussed, and therefore most of the literature employed in this review will be related to cyber security in organisations. However, this chapter also highlights that psychology and usable security have influenced cyber-security research outside of the organisational context, and how this is also considered critical for a holistic understanding of cyber-security perceptions and behaviours.

This literature review will discuss some of the most prominent psychological theories of risk perception and behaviour change used in cyber-security research. Such theories include Protection Motivation Theory (Prentice-Dunn & Rogers, 1986), the Extended Parallel Process Model (Witte, 1996) and the Theory of Planned Behaviour (Ajzen, 1985); these theories will be discussed in sections 2.2.2, 2.2.4 and 2.2.6 respectively. This review will look at the practical ways researchers have previously used risk communication to change perceptions and behaviour. Within each relevant section, this review will summarise research that has applied social psychological theories to the field of cyber security and cyber-security research within organisations, as well as highlight some gaps in the current research. The review will also look at the notion of cognitive biases and perceptions, such as the optimism bias, and how this research has been applied to understand the user in cyber security.

These three theories were chosen for this research for a number of reasons. Firstly, the aim was to choose psychologically based behavioural theories. Psychological approaches to behaviour aim to encompass perceptual antecedents to behaviour and, in this way allow, for a holistic and deep understanding of the perception and behaviour process (Ajzen, 1985;

Prentice-Dunn & Rogers, 1986; Witte, 1996). Secondly, research has consistently demonstrated TPB and PMT to apply to cyber security, with their constructs having been correlated to types of cyber-security behaviour (Blythe et al., 2015; Lebek et al., 2013). The EPPM was created as an extension of PMT, with evidence supporting the theory beginning to be demonstrated in the cyber-security field. Therefore, in the current research, it was decided to include this theory to explore whether the original PMT model and the EPPM applied to the present research. Since the current research does not aim to test correlations between constructs of the respective theories, or how individual constructs influence and impact behavioural intention or cyber-security behaviour, it was important to use theories that had such supporting evidence already. In this way, the current case study would be able to look at how, and to what extent, the concepts underpinning these psychological theories apply to cyber-security behaviour and perceptions within organisations using a qualitative case-study methodology.

Other theoretical models are also used consistently within behavioural cyber-security research (Lebek et al., 2013), such as General Deterrence Theory or the Technology Acceptance Model. Such theories have great merit, and it should be made explicit that their exclusion in the current research was not down to a lack of importance. General Deterrence Theory is situated within criminology and therefore has proven useful in areas of cyber security, such as understanding cyberbullying and how such behaviour might be discouraged (Zhang, Wakefield & Leidner, 2016). General deterrence theory has also been successfully used to shed light on cybercriminal behaviour (Bhattacherjee & Shrivastava, 2018). The Technological Acceptance Model on the other hand has evolved to become a key model in understanding predictors of human behaviour toward potential acceptance or rejection of the technology (Marangunić & Granić, 2015). These theories use cases therefore were deemed less applicable to the aims and research questions of the current research, which focuses on non-criminal areas, and are not directed specifically to technological adoption. The General Deterrence Theory or the Technology Acceptance Model were therefore deemed outside the scope of the current research.

Secondly, in section 2.5, the literature will look at the field of usable security, and how the present research is supported by and substantiates the previously discussed psychological

theories and research within cyber security. This section will focus on how research has highlighted the need to understand the user and use this knowledge to advance security, rather than force the user to comply with security notions that do not work in practice (Bada et al., 2019). Furthermore, this section will highlight that more research is needed that encourages the idea of the employee or the user as a solution to cyber security, rather than a hindrance (Zimmermann & Renaud, 2019). Evidence that demonstrates the importance of both the employee and the manager in the cyber-security process will also be highlighted in this second section (Kirsch & Boss, 2007). The literature review will look at the three waves of usable security (Bødker, 2006), and the applications of this research to organisational cyber security.

The literature review will then demonstrate how researchers have used psychology and usable security research to examine specific cyber-security behaviour of employees within organisations (Pattinson et al., 2012). Works highlighting the current gaps in the surrounding literature will also be noted. This chapter will then examine the current standing of research within the human factors area of cyber security inside organisations and summarise the gaps in the research. Finally, the impact of the COVID-19 pandemic on cyber security will be considered regarding the newly emerging literature. Through discussions of previous research, we can understand how cyber-security culture, behaviours and individual perceptions and biases have been understood previously in the context of organisations, and how new research may be able to supplement this.

2.2 Psychological Theory and Research

Addressing the role of the human in cyber security is becoming ever more important; as systems are becoming increasingly technically secure, threat actors are shifting their focus towards exploiting the vulnerabilities in the human side of cyber (Joinson & Steen, 2018). A large body of HCI research has looked at individuals' perceptions of cyber-security threats (Furnell et al., 2007; Huang et al., 2011; Ur et al., 2016; Van Schaik et al., 2017; Weirich & Sasse, 2001) and has applied psychological theories to understand such perceptions and

change behaviour. These studies demonstrate that concern can be raised about the state of awareness and the accuracy of such perceptions. Attitudes and perceptions of information security threats directly impact security behaviours (Ifinedo, 2012). Furthermore, attitudes and perceptions themselves can be affected by many different factors or combinations of such factors, such as inherent inaccurate perceptions of personal risk, demographics, such as age, schooling, income, sex, and race (Savage, 1993), heuristics (Tversky & Kahenman, 1974) and many more. Hence this body of research is important for anyone trying to understand and change cyber security user behaviour (Bada et al., 2019).

Persuasive communication theories generally attempt to understand risks and how people cope with them as well as offer suggestions for how to change 'unhealthy' behaviours. There is a wide range of definitions and interpretations of the concept of risk perception, human responses to risk and behavioural change that have been accepted and published within the psychological literature (Haimes, 2009). Risk communication involves one party trying to get another party to understand a threat and change their actions towards this risk (Breakwell, 2014; Plough & Krimsky, 1987). However, it is unusual that risk communication will only involve two parties. The use of risk communication has been studied in a variety of disciplines such as public health behaviours (Berry, 2004), food risk (Lofstedt, 2006), aviation (Witte, 1995), drunk driving (Elder et al., 2004) and disaster response (Eisenman et al., 2007) and has many practical applications. Such research has influenced many different theories and models of risk communication, such as Protection Motivation Theory (Palenchar & Heath, 2007; Prentice-Dunn & Rogers, 1986; Witte, 1995) and, in turn, has been looked at through the lens of these theories. Given the success of such theories in providing insight into other risk-related fields, in the last few decades, this research has also focused on the application and effects of risk communication on cyber security in organisations. Much of the social psychological research applied to cyber security has only focused on a few areas, such as fear appeals (McCrohan et al., 2010). This section of the literature review will first outline some risk communication theories. Secondly, the literature review will look at the evidence used to support the theories generally and specifically in relation to cyber security.

2.2.1 Theories of Risk Communication and Behavioural Change

Through its decades of research and insight into risk communication and human behaviour, psychology has a crucial and valuable function in mitigating risky cyber-security behaviours (Whitty et al., 2015). Different theories incorporate how risk is best communicated and how individuals receive it. Such theories have developed as different industries and institutions have had the concepts of such theoretical models tested on them (Fischhoff, 1995). Typically, it is hard to come to a clear conclusion about what exactly needs to be communicated to a target population in order for them to change their behaviour. Moreover, not everyone reacts to risk communication in the same way. It is also often difficult to gauge the success of such communications (Morgan et al., 2002). Theories looking at risk communication generally include an element of highlighting a risk to the audience, thereby creating some form of fear (even if low level). They also look at how people perceive the threat and whether they feel they have the ability to cope with it.

In their basic form, fear appeals are a type of risk communication that relies on the ability to highlight a particular threat or risk to change individuals' behaviours and attitudes (Williams, 2012). The 'ideal' structure of a fear appeal has changed little during the last few decades of research; firstly, a threat or risk is presented in a message, usually in the form of a behaviour change campaign, and secondly, a protective action is suggested (Ruiter et al., 2001). For example, in the context of cyber security, the risk messaging might be 'you are at risk of falling victim to a phishing email', and the protective action might be 'make sure to read all email addresses carefully and report anything suspicious'. Scholars have researched fear appeals for over 60 years and have identified three key independent variables of this concept: perceived efficacy, perceived threat, and, of course, fear (Witte & Allen, 2000).

Perceived threat, first identified as important by Rogers (1975), is composed of the concepts of perceived vulnerability to the threat (how relevant you think the threat is to you) and the perceived severity of this threat (the significance of the consequences of this threat) (Witte, 1996). Fear is hypothesised to be directly related to the perceived threat, in that the higher the perceived threat, the more fear that is experienced. Perceived efficacy is composed of two dimensions: perceived self-efficacy (the belief that the recommended response can be

performed) and perceived response efficacy (the belief that the recommended response works to deter the threat). Perceived efficacy and perceived threat are proposed to interact differently based on the given theory; these interactions are therefore discussed in depth in the respective theoretical sections. Generally, researchers in this area manipulate the strength of fear or feelings of efficacy to study the fear reactions of participants. Many theories include an element of fear appeals, including Protection Motivation Theory (Rogers, 1975) and The Extended Parallel Process Model (Witte, 1992). These are not the only two theories including elements of fear appeals, for example, the Parallel Response or Process Model (Leventhal, 1970). However, this theory has limited the scope for this literature review, as the theories identified for the current research are those that have been widely used in studies attempting to understand cyber-security behaviour (Herath & Rao 2009b; Ifinedo, 2009; Siponen et al., 2010; Vance et al., 2012).

2.2.2 Protection Motivation Theory (PMT)

Rogers (1975), and later Prentice-Dunn and Rogers (1986), originally proposed PMT as a framework to provide conceptual clarity to the notion of fear appeals (Prentice-Dunn & Rogers, 1986). Additionally, PMT was developed to create a more general model of persuasive communications with a significant focus on the cognitive processes which mediate behavioural and attitudinal change (Norman et al., 2005). Research on PMT has analysed and evaluated the persuasiveness of different behavioural change campaigns and communications (Cismaru, 2006; Mulilis & Lippa, 1990). These campaigns refer to national behaviour change campaigns, for example, to encourage individuals to stop smoking, drive at the speed limit, and smaller organisational policy-based campaigns, for example, encouraging employees to shred important documents. PMT has been used as an influential social cognition model to predict health behaviour (Milne et al., 2000; Pechmann et al., 2003). There have been recent attempts to apply PMT to new avenues of research, such as cyber-security behaviours (Doane et al., 2016).

PMT proposes two independent appraisal processes: coping appraisals and threat appraisals. These can arise from various environmental and intrapersonal sources of information that

are seen to be a threat (Norman et al., 2005). Threat appraisals focus on the source of the perceived threat and the factors that may increase or decrease dysfunctional responses (such as avoidance and denial). As previously mentioned, two concepts contribute to the threat appraisal; beliefs about one's perceived vulnerability to the threat and the severity of the threat (Norman et al., 2005). Fear is also an influential factor; greater levels of fear will be aroused if individuals perceive themselves as vulnerable and the threat to be severe (Prentice-Dunn & Rogers, 1986). The concept of coping appraisals focusses on the possible responses to the threat an individual can take to cope with the threat and perform an adaptive response. The belief that the recommended behaviour will reduce the threat (response efficacy) and the belief that one can perform the recommended behaviour (self-efficacy) increase the likelihood of an adaptive response (Norman et al., 2005). Protection motivation is thereby a product of these two appraisals and is positively influenced by high levels of perceptions of severity, vulnerability, self-efficacy and response efficacy. Protection motivation is also a negative function of any perceived rewards of maladaptive responses and the possible costs of the suggested adaptive behaviour. Therefore, protection motivation, which is proposed to be highly related to behavioural intention, is seen to direct protective behaviour.

There has been ample research on PMT in two main areas. The first area of research manipulates the individual components of PMT in persuasive contexts and measures the outcomes. The second primarily uses PMT to predict health behaviour (Norman et al. 2005). A few systematic reviews and meta-analyses have attempted to synthesise such evidence and provide a commentary on the effectiveness of PMT. Floyd et al. (2000) conducted the first meta-analysis of PMT studies. The review includes 65 studies, and the results showed a moderate mean overall effect size, with self-efficacy presenting the highest effect size. Furthermore, it was found that, in general, increases in threat vulnerability, threat severity, response efficacy and self-efficacy aided adaptive intentions and behaviours. On the other hand, decreases in maladaptive response rewards and adaptive response costs increased adaptive intentions or behaviours (Floyd et al., 2000). Overall, the results supported the model, with self-efficacy providing the strongest predictions of protection motivation. A second meta-analysis later supported these results (Milne et al., 2006). This subsequent meta-analytical review assessed associations between threat and coping appraisal variables

with intentions to perform behaviours and all other components of the model. PMT was found to be useful in predicting concurrent behaviour. However, the coping-appraisal component of the model was found to have greater predictive validity than the threat-appraisal component. Furthermore, in the context of public health campaigns, several meta-analyses, consisting of over 100 studies combined, have shown support for PMT and fear appeals. These meta-analyses find that high amounts of fear combined with high efficacy led to the most significant amounts of behaviour change, whilst high fear with low-efficacy messages produced defensive responses (Floyd et al., 2000; Witte & Allen, 2000; Peters et al., 2013; Tannenbaum et al., 2015).

Despite general support for PMT, it has also faced some criticisms from scholars. PMT has been criticised for failing to explain and account for why people reject risk communication messages (Witte, 1995). Furthermore, although much research demonstrates that greater fear yields greater attitudinal change, behaviour has generally shown a less consistent relationship with fear (Dillard, 1994). Across different studies, behaviour appears to vary as a function of numerous other variables, such as personality constructs (Leventhal, 1970). Hence, since a primary of PMT, especially in relation to risk communication and persuasion, is to help motivate people to change certain behaviours, the application of PMT becomes less useful (Dillard, 1994). However, although it may not be a clear-cut and direct effect, it is evident that fear does play a meaningful role in the persuasive process. Furthermore, meta-analytical findings seem to lend strong support for the role of fear and the persuasiveness of fear appeals (Peters et al., 2013; Witte & Allen, 2000).

2.2.3 The Application of PMT to Cyber Security

Over the last decade, cyber-security research within organisations has drawn on the aforementioned risk communication and persuasion theories. PMT, as one of the most influential models of persuasive communication and predictors of behaviour, has been used widely to inform research in this field (Bulgurcu et al., 2010; Herath & Rao, 2009b; Pahnila et al., 2007). The PMT model has been used to investigate and understand cyber-security

awareness and training campaigns within organisations in relation to the best methods to use to change behaviour and to understand employee reactions to threats.

Herath and Rao (2009b) investigated motivational factors embedded in PMT to explain compliance behaviour in employees within 78 organisations. Results showed that threat perceptions about breaches in security, response perceptions of response efficacy, self-efficacy, and response costs affected attitudes towards organisational policy. This demonstrates the value of using PMT to predict cyber-security attitudes. Bulgurcu et al. (2010), in a similar study, correspondingly established that employees' intention to comply with cyber-security policy is significantly affected by normative beliefs, attitudes and self-efficacy. However, creating awareness and intention is not necessarily enough to drive behavioural change (Bada & Sasse, 2014). Tsai et al. (2016) further found that PMT factors could be used to predict an individual's online safety intentions. Meta-analyses, systematic reviews and literature reviews have also been conducted to analyse the role of the different components of PMT, along with cognitive and cultural biases about the adoption of cyber-security policies. In their paper, Tsohou et al. (2015) combined and analysed many available papers (such as Herath and Rao (2009b), Ifinedo (2009), Siponen et al. (2010), Vance et al. (2012) and many others previously discussed in this section) looking at factors affecting compliance in cyber security. It was found that many PMT constructs had an influence on cyber-security compliance, and the authors were able to make recommendations for cyber-security awareness campaigns based on such findings. These recommendations, for example, include informative based communication styles and point to the idea that identifying biases should be a prerequisite to addressing them.

Studies in the cyber security domain have also researched fear appeals as a broad concept for behaviour change. Johnston and Warkentin (2010) investigated the use of a fear appeal, based on PMT and technology adoption theories, to influence participant behaviours in relation to spyware. Results demonstrated that fear appeals do impact end-user behaviour and intentions to comply with recommendations but that such impacts are not uniform across all employees. However, subsequent research has highlighted inconsistencies in results (Warkentin & Siponen, 2015; Weirich & Sasse, 2001) regarding the effectiveness of fear appeals in this context and the misapplication of PMT to cyber-security research

(Warkentin & Siponen, 2015). Boss et al. (2015) assert that very few PMT-based cyber security studies have experimentally manipulated the different components of fear appeals, while even less have pointed to fear as a key component of PMT. Research has also suggested that people are immune to cyber security-related fear appeals and has demonstrated negative and counterproductive impacts (Weirich & Sasse, 2001).

Furthermore, many studies which cite PMT as the foundational model for the research focus on fear. It should be noted that there are many other aspects of PMT worthy of further attention, such as efficacy and motivation (Menard et al., 2017), as well as biases that may arise owing to maladaptive thinking strategies. Menard et al. (2017) demonstrated that motivation is a worthwhile feature to focus on by creating security messages which centre on the constructs that make up either PMT or Self-Determination Theory (a theory of human motivation). Self-Determination Theory posits that individuals, in order to have the self-determination needed to achieve psychological growth individuals must feel autonomous, competent and experience a sense of belonging and attachment to others. Results demonstrated that security messages appealing to individuals' motivation had a significant positive impact on an individual's intention to adhere to security behaviours. This, therefore, shows that in the context of cyber security, motivation could be an alternative factor to fear (Menard et al., 2017).

Blythe et al. (2015) also investigated factors that influenced the compliance of individuals with cyber-security policies in the workplace. The study demonstrated seven broad factors that influenced security compliance: self-efficacy, social influence, attitude towards the task, perceived susceptibility, perceived severity of the threat, security responsibility, response efficacy and response cost. Furthermore, the influence of the factors depended on the security behaviour in question. It was argued that the interplay between all these factors influences the degree to which employees engage in security behaviours and that an extended PMT model with other security-contextual factors may be able to explain additional variance in cyber-security behaviour. This demonstrates that cyber-security compliance is complicated as different security behaviours are motivated by different factors and to different degrees (Blythe et al., 2015). It was suggested that future awareness campaigns should focus on more specific cyber-security behaviours.

Many other studies have further demonstrated the impact and usefulness of using PMT as a model to assist in the design of cyber-security training and awareness campaigns that do not use fear-based methods. Such methods have been found to be effective. For example, coping messages have been found to be more effective than threat appeals (van Bavel et al., 2019) and awareness of security policies have been shown to positively influence the competency of cyber-security tasks (Li et al., 2019). Psychology and usable security research have also been applied to understanding cyber-security awareness and training, this will be discussed in more detail section 2.7.1 of the literature review. More recently, PMT has been used to assist in designing interactive games to encourage privacy-protecting behaviour (Williams et al., 2019a; Williams et al., 2019b), has been applied to mechanisms to protect against insider attacks (Posey et al., 2011; Zuwita & Rahmatullah, 2021), and understand responses to phishing attacks (Bayl-Smith et al., 2021).

However, there are also many criticisms of the use of PMT methods to influence cyber-security awareness campaigns. It has been argued that threats to data and systems do not carry the same relevance as threats related to healthcare (which was what this model was originally designed for) that directly affect the self (Warkentin & Siponen, 2015). However, with the increasing number of cyber-attacks relating to private information and data and with companies increasingly placing penalties on employees who break compliance or even make mistakes (Herath & Rao, 2009b; Tsohou et al., 2015), cyber security and cyber threats arguably do have individual consequences to employees. The research above also focusses on compliance within organisations, as has been the general trend for applying PMT to cyber security within organisations. Previous cyber-security research tends to focus on the human as a negative, with awareness and behaviour change campaigns focussing on constraining employees rather than attempting to understand why employees do not or cannot comply and fit policies around usability (Goo et al., 2014; Hughes-Lartey et al., 2021; Lowry & Moody, 2015; Sabillon, 2022).

In 2021 a systematic review of PMT and cyber security 67 studies were identified (Haag et al., 2021). This review aimed to look at the application of PMT to Information Systems (IS) and compare this with its application to psychology and identify areas where PMT is yet to be

applied to IS research. The findings of the review demonstrated ways in which PMT has previously been useful in cyber security, finding that PMT based cyber-security research has primarily been focussed on the fear appeal aspects of PMT and suggests five broad recommendations for further research. The first recommendation is that researchers should 'Measure the Level of Concern about IS Security Threats'; researchers should not assume that subjects experience the cyber-security threat as concerning but should confirm experiences with research (Haag et al., 2021). Secondly, researchers should 'Measure Confidence in Relationship Between Protective Behaviour and IS Security Threat Reduction'. Meaning that researchers should look to see if performing 'recommended protective behaviours' such as strong passwords and the reduction of information security threats exists. Thirdly, cyber-security researchers need to find a way to personalise cyber-security threat messages in order for them to be persuasive, as not all participants are the same and should not be treated as such. They propose different manipulations, such as source credibility, empathy, and personality variables. Fourth, research needs to study the role of maladaptive coping (the methods a person uses, both consciously and subconsciously, to attempt to reduce cyber security threats, but in an ineffective or 'unhealthy' way) in the organisational context when corporate cyber security is threatened. This could include, for example, coping biases such as the optimism bias (thinking a threat is more likely to happen to others than yourself) and fatalistic thinking (thinking a threat is inevitable and so not acting to reduce the threat). These concepts are defined in detail later in sections 2.3.1 and 2.3.2 respectively. Lastly, the authors recommend that future studies should examine individual differences in the way people process cyber-security threats (Haag et al., 2021).

As evident from this subsection, PMT has previously been used within the field of cyber security, particularly in studies pertaining to research that has tried to explain rather than understand security behaviours. However, its applicability in existing research has generally been in the context of cyber-security awareness campaigns within organisations and has been survey-based or quantitative in nature. Moreover, PMT is still under-researched in certain areas, such as within qualitative research, and has not been commonly considered alongside usable security literature. There is a significant paucity of cyber security-related scholarship using PMT to understand behaviours. As such, the majority of existing PMT research in cyber security rests upon attitude surveys. Alternatively, if not, the research

includes an assortment of different organisations, allowing for a variety of influencing factors. Although this research is valuable, there is a growing need for studies to explore the in-context, qualitative details of how people construct relevant beliefs. This is important to gain a deeper understanding of how individuals comprehend cyber-security threats to inform cyber-security awareness campaigns, generate effective cyber-security policies and increase compliance. Furthermore, there are specific research areas where PMT should be applied, such as understanding maladaptive coping responses within organisations.

2.2.4 The Extended Parallel Process Model (EPPM)

The EPPM is one of the latest developments in the area of fear appeals. The EPPM integrates and builds on previous models to explain when fear appeals work when they do not and why (Witte, 1996). Such models include PMT, the parallel process model (Leventhal & Trembly, 1968) and drive models (Hovland et al., 1953). The EPPM has been used and tested in different contexts, such as fear appeals in AIDS prevention campaigns (Witte, 1994), fear appeals about meningitis to students (Gore & Bracken, 2005), and to assess local public health agencies' willingness to respond to pandemic influenza (Barnett et al., 2009).

According to the EPPM, fear-producing messages and campaigns may initiate two appraisals; an appraisal of the presented threat and an appraisal of the response recommended in the message (Witte, 1996). These two appraisals then initiate one of three responses: rejection of the message, acceptance of the message or no response to the message (Witte, 1992). For perceived threat, individuals additively appraise how severe the threat appears to be and their personal vulnerability to the threat (Witte, 1996). The theory suggests that if a person believes their susceptibility to the threat and the severity of the threat to be low, then they will not be motivated to respond (Witte, 1992). If perceptions of the threat reach a particular increased level, then the theory suggests that people will feel motivated enough to begin the second appraisal; weighing up the efficacy of the recommended response with the perceived strength/severity of the communicated threat (Witte, 1996). The more heightened the level of fear and threat, the more likely people are to have some kind of response to the presented threat. People then generally react with one of two responses; become motivated to act to

control their fear (fear control) or become motivated to control the danger of the threat (danger control). This will be determined by the amount of perceived efficacy (made up of both self-efficacy and response efficacy).

The secondary appraisal process in the EPPM theory is the efficacy related appraisal. Here, people appraise the perceived efficacy based on the previous appraisal of the perceived threat (Witte, 1992). If the perceived efficacy is greater than the perceived threat, people will engage in danger-control processes, whereby they will take steps to avert the threat by adopting the recommended action (Witte, 1996). Hence, if there is high perceived threat and high perceived efficacy, people will be motivated to engage in protection motivation and danger control processes (Witte, 1996), and motivate people to carefully think about the recommended response to the message and take steps to perform this response. However, if perceptions of the threat begin to exceed the perceptions of efficacy, people will shift to fear control processes, where, instead of thinking about the threat, people will act to control their levels of fear (Witte, 1996). Fear control is thought to be engaged in if people do not feel they can engage in the recommended protective behaviour because it is too hard, takes too much time, is too costly, or they do not believe it will work. Therefore, low perceived efficacy and high perceived threat promote defensive behaviours incorporating elements of denial. Overall, the EPPM hypothesises that individuals will contemplate and weigh up perceived efficacy against perceived threat (Witte, 1996). The EPPM does not consider individual differences, such as traits and attitudes, to play a part in influencing outcomes; they may, however, influence individual perceptions, which are mediated by individual perceptions of efficacy and threat.

Like PMT, there is significant evidence evaluating the EPPM, mainly concerning health campaigns but across a variety of methods and populations. For example, one study by Witte (1994) used the EPPM to analyse the cognitive and emotional means underlying the possible success and failure of fear communications and campaigns related to AIDS prevention. This study provided overall support for the model, finding that cognitions that lead to the success of the AIDS fear appeals (behaviour or attitude changes) happened through the danger control processes, as described in the model. On the other hand, high fear leads to fear appeal failure (defensive/avoidance behaviour) via the fear control processes, as described in

the model (Witte, 1994). The EPPM is also supported by Witte and Allen's (2000) influential review on fear appeals and their implications for public health campaigns. More recently, Birmingham et al. (2015) found the EPPM to be successful in aiding the design of effective interventions in motivating colorectal cancer screening.

Furthermore, studies looking at fear appeals in health campaigns have also investigated specific aspects of the model. Ruiter et al. (2004) investigated the EPPM's proposed reactions to fear appeals (danger or fear control) about breast cancer. Participants read high or low threat messages about breast cancer, followed by a persuasive message that recommended the protective action of conducting a breast self-examination. It was found that, in general, presenting participants with a high threat of breast cancer motivated more danger control actions than fear control compared to low threat messages. However, it was also found that this result was mediated by participants' need for cognition (Ruiter et al., 2004). Participants with a high need for cognition, and those with a tendency to cognitively tackle threats presented to them, were more willing to accept the recommended action than those with a low need for cognition. This study, therefore, demonstrates the influence of individual differences on responses to fear appeals.

However, although the EPPM's theoretical concepts are soundly developed (Popova, 2012), the theory has been criticised for lacking operational consistency in relation to a few of its constructs (Popova, 2012). For example, the concept of fear differs depending on the study, with some treating fear as to how 'frightened' participants are as a primitive concept (Smith et al., 2007), in that it is assumed to be understood by the author. In contrast, others explicitly define fear within their study (Gore & Bracken, 2005). Furthermore, not one of the constructs proposed by the EPPM has received complete support from all research (Popova, 2012). For example, McMahan et al. (1998) looked at risk communication on electromagnetic fields (EMFs) and the uncertain hazards they present to individuals. The study found that there was no difference in behavioural responses to electromagnetic field risk messages between those with low perceptions of efficacy, regardless of whether individuals perceived the threat as low or high (McMahan et al., 1998). Despite these criticisms, the EPPM has been demonstrated to be useful in guiding risk communication campaigns, especially those

related to health behaviour, and remains one of the latest developments in theories that seek to explain the role of fear in the communication context (Popova, 2012).

2.2.5 The Application of the EPPM to Cyber Security

Despite the previously mentioned broad research on fear appeals being applied to a cyber-security context, there is less research on the application of the EPPM model to cyber security compared to PMT. This is perhaps unsurprising given that the PMT model is more heavily studied in other fields, and the cyber-security field is relatively new. However, any application of fear appeals to this area is likely to have some grounding in theories such as EPPM. For example, Warkentin and Siponen (2015) found that when fear appeals included references to sanctions, cyber-security fear appeals were found to be efficacious in enhancing employee intentions to comply with cyber-security policies.

Other studies have directly used the EPPM within the organisational cyber-security context. Zhang and Borden (2020) used the EPPM model to demonstrate that the appraisal process and emotional arousals are an essential part of people's risk message processing in relation to cyber security. Chen et al. (2021) used the EPPM model to understand inconsistent employee compliance with cyber security successfully. Similarly, Masuch et al. (2021) used the EPPM model to understand the influence of threat and efficacy on cyber-security behaviour. Results showed, similarly to some of the findings regarding PMT, that participants who received a low threat message were less afraid and more likely to deal with a cyber security issue but were not as confident as people who perceived a significant threat. Participants who felt that they had little protection against ransomware were more fearful and therefore dealt with the topic more defensively, such as avoiding the threat. Conversely, they also had the intention to behave safely. Other studies have further supported the idea using this model that coping appraisals play a more dominant role in promoting adaptive security behaviours, while fear elicits both maladaptive security behaviours additionally (Chen et al., 2021; Chen, 2017).

2.2.6 The Theory of Planned Behaviour (TPB)

Theories without a primary focus on fear, such as those looking at persuasion and decision making alone, can also be applied to the area of risk communication. Such theories are significant in the context of cyber-security research given that, while some cyber security researchers advocate the use of fear appeals (Warkentin & Siponen, 2015), other researchers consider them to be counterproductive and are concerned about the ethics of using fear as a method for communication in research and situ (Lawson et al., 2016; Renaud & Dupuis, 2019).

Since TPB was introduced (Ajzen, 1985) as a model that sought to explore how attitudes predict behavioural intentions, it has become one of the leading models for the prediction of social behaviour in humans (Ajzen, 1991; Azjen, 2002). The theory has been used and applied to many different areas. These areas include, but are not limited to, leisure intentions (Ajzen & Driver, 1992), driving behaviour (Parker et al., 1992) and health behaviour (Godin & Kok, 1996). TPB aims to explain an individual's intentions to perform a specific behaviour with risk perception already implicitly accounted for in the classical TPB framework. Therefore, TPB may be useful in helping to explain how individuals develop intentions to perform an adaptive response to a threat presented to them.

TPB proposes that the intention to perform a specific behaviour can be predicted accurately by three kinds of considerations (Ajzen, 1985). These are behavioural beliefs (beliefs about the probable outcomes of the possible behaviour and the assessments of these outcomes), normative beliefs (beliefs about the possible expectations of other individuals and one's motivation to fulfil these expectations) and control beliefs (beliefs about the existence of possible factors that may enable or impede one's ability to perform the behaviour and the perceived influence of these factors). Behavioural beliefs then work as antecedents to attitudes towards the behaviour by producing a positive or negative attitude. Normative beliefs produce subjective norms (perceived social pressure), and control beliefs produce perceived behavioural control. Perceived behavioural control relates to an individual's perceived ease or struggles in performing the behaviour. In combination, the subjective norm, attitude toward the behaviour and perceived behavioural control lead to the creation

of a behavioural intention (Ajzen, 1985). The theory suggests that the more favourable the attitude and subjective norm, and the better the perceived behavioural control, the greater the person's intention to perform the particular behaviour. Intention is the immediate antecedent of behaviour. Hence, if there is enough actual individual control and perceived behavioural control over the behaviour, an individual will carry out the behaviour as intended (Ajzen, 1985). In the context of cyber security then, and cyber-security compliance behaviours within organisations, the TPB suggests that if an employee perceives that they have sufficient capacity to complete the security task, have a favourable attitude towards performing it, and observe a norm where other people in the organisation are also actively performing the practice, or know that a practice is expected of them, they will likely comply with cyber-security policies (Pham et al., 2017).

The TPB has been greatly popular and has been applied to understand a large amount of social behaviour and behaviour change campaigns. However, the theory has been subject to criticism (Ajzen, 2011). Similar to many models aiming to predict behaviour, the TPB is limited in its predictive validity. Studies show that measures of attitude towards a behaviour, subjective norm, perceived behavioural control, intention and behaviour exhibit medium correlations and that these results differ dramatically across different studies (McEachan et al., 2011). Therefore, factors not included in the model seemingly have a great influence on the ability of the model to predict a given behaviour. Furthermore, another significant criticism in the literature is that TPB is too rational in that it does not take into account possible cognitive processes that are shown to bias human intentions and behaviour (Ajzen, 2011). However, although TPB does focus on the controlled features of behavioural decision making, it is explicit about this, and the theory is primarily concerned with goal-directed behaviours and conscious processes. This focus should not, therefore, be misinterpreted as the theory positing a rational actor who works in an unbiased way regarding behavioural decisions (Ajzen, 2011). Notwithstanding these criticisms, the TPB has been and continues to be of great influence in the psychology of predicting behaviours, with applications to many areas, including that cyber security (Bulgurcu et al., 2010). Researchers now argue that, in a similar vein to PMT, we do not need any more correlational studies of the TPB as the relationships between constructs in the TPB are known, as are the insufficiencies of the theory. Rather, research in this area needs the model to be applied and theoretically

developed to explain behavioural phenomena to better help people change their behaviour and to help those who design and deliver interventions to help people to do so.

2.2.7 The Application of the TPB to Cyber Security

Despite the popularity of TPB in other domains, such as health-related behaviour (Conner & Sparks, 2005; McEachan et al., 2011), the theory has only a few studies looking at its applicability to cyber security within an organisational context. Bulgurcu et al. (2010), in a study looking at both PMT and TPB, found factors from both theories, such as self-efficacy and normative beliefs, to be influential in employee compliance with cyber-security policies. Sommestad et al. (2015) found TPB to predict compliance with cyber-security policies well, especially when the element of anticipated regret was added to the model. Similarly, Ifinedo (2012), in a survey of 124 business managers and IS professionals, looked at both PMT and TPB elements in how they influenced participants' intentions to comply with cyber-security policies. It was found that both PMT and TPB concepts, such as attitude toward compliance and subjective norms, influenced behaviour. Furthermore, the concept of security champions (employees who demonstrate good cyber-security behaviour by example) stems from the idea of perceived social pressure (Gabriel & Furnell, 2011), which features in TPB. More recently, a meta-analysis investigated factors influencing cyber-security policy compliance behaviour based on TPB and demonstrated the main TPB components to significantly influence behavioural intention with reference to security policies (Kim & Mou, 2020). Thus, although TPB has had some influence in understanding the human in cyber security, like with all of the theories discussed in this report, there is room for more research on its applications.

Moreover, in accordance with the TPB's main argument on the relationship between intention and behaviour, most of the aforementioned studies used security intention as the dependent construct and argued that intention would lead to actual behaviour (Sommestad et al., 2014). Meaning that such studies did not record actual behaviour. The main reason for this is that monitoring and recording cyber-security behaviour in an organisation is difficult (Crossler et al., 2013). For instance, security behaviour can be recorded through

technological means, such as cameras, or through managerial monitoring of user behaviour (Pham et al., 2017), or studies can rely on self-report questionnaires and reports from interviews. However, access to cyber information sources, such as employees themselves, detailing user security actions in organisational contexts can be difficult to obtain for research purposes due to confidentiality concerns from the organisation, cost (Warkentin et al., 2012) and difficulties in the current climate gaining in-person access due to COVID-19.

2.3 Heuristics and Cognitive Biases

As noted above, certain combinations of the PMT constructs may lead to maladaptive coping responses. Unrealistic optimism and other cognitive biases and heuristics have been found to act as a coping response (Scheier & Carver, 1985) and a means to understand risks (Peters et al., 2006), such as the risk of cyber-security threats. Within the discipline of psychology, many studies and theories have explored the effects of hundreds of biases and heuristics on human judgement (Gilovich et al., 2002). The foundations of this research rest on the idea that human decision-making and judgement, in times of uncertainty, rely on simplifying heuristics, or mental shortcuts, to reduce cognitive load (Kahneman et al., 1982).

In their original work, Tversky and Kahenman (1974) identified three main types of heuristics that they believed individuals employ when making judgements under uncertainty, and that can give way to biases and errors in decisions. First the availability heuristic, where people make judgements about the likelihood of an event happening based on how easily they bring an example to mind (Harvey, 2007). In relation to cyber security, this might resemble focusing personal security efforts on threats regularly ``witnessed'' through news or other popular sources of information. Secondly, the representativeness heuristic is used when judging probabilities. This assumes that we make judgements about the probability of an event based on a previous idea that already exists in our minds (Harvey, 2007). In cyber security, this might be making a judgement about the likelihood of someone being a victim of a threat based on their personal characteristics, such as their job. Therefore, if individuals do not believe they fit this heuristic, they would not view themselves as likely victims. Thirdly,

the anchoring and adjustment heuristic relates to individuals relying on an initial piece of information or value to make follow-on judgements, with subsequent information being adjusted to fit the initial belief (Harvey, 2007). For example, individuals might base all judgements about the validity of an email on one phishing email they have previously seen. These three heuristics have a large research backing, and the influence of this approach has created a plethora of different heuristics researched in multiple fields. However, only a few (Gambino et al., 2016; Vishwanath, Harrison & Ng, 2018) heuristics have been empirically researched in the context of HCI. Though many, such as the availability heuristic, have been proposed to impact perceptions in this domain (Ashenden, 2018; McAlaney & Benson, 2020; Tsohou et al., 2015).

Following this initial research by Tversky and Kahneman (1974), scholars in psychology have demonstrated how a plethora of biases and heuristics can influence human judgement, thus, no longer fitting into the three categories defined by Tversky and Kahneman. A review conducted in 2015 identified 19 of these biases applicable to the medical domain alone (Blumenthal-Barby & Krieger, 2015), with the optimism bias being one of the most prevalent and heavily quantitatively researched.

2.3.1 The Optimism Bias

The optimism bias refers to a perception of one's personal vulnerability; a tendency of individuals to generally believe that negative events are more likely to happen to others than themselves or that one has a lower risk than average (Weinstein, 1980). Researchers have investigated and documented this bias in over a thousand studies (Shepperd et al., 2015) in many different and diverse disciplines for an array of risks. For example, natural disasters such as earthquakes (Trumbo et al., 2011), physical health risks such as cancer (Jansen et al., 2018) and cardiovascular disease (Masiero et al., 2018), privacy concerns (Baek et al., 2014), and other areas such as future marriage predictions (Helweg-Larsen et al., 2011) and job prospects (Spinnewijn, 2015).

The optimism bias can be located within wider research that has looked at self-serving or self-enhancing biases (Weinstein & Klein, 1996). Self-serving biases focus on the premise that people believe that they are better than others and describe the tendency of individuals to interpret and justify outcomes in a way that has favourable outcomes for the self (Blaine & Crocker, 1993). Research provides unambiguous support for the existence of self-serving biases and that they are widespread (Blaine & Crocker, 1993). Self-serving biases include the self-serving attributional bias, whereby people are more likely to attribute positive events to the internal self and attribute negative events as attributable to other causes outside of the self (Mezulis et al., 2004).

The optimism bias is easy to demonstrate, especially in relation to risk comparisons. The optimism bias can be confirmed if a person believes their own risk to be lower than their peers; this is what is known as unrealistic comparative optimism (Shepperd et al., 2015). This can be operationalised as a person incorrectly judging that their own risk is less than that of others. For example, one study, to determine unrealistic optimism, compared participants perceived risk to their objective risk about their chances of getting breast cancer (Waters et al., 2011). Participants were asked, "compared to the average woman your age, would you say that you are more likely to get breast cancer, less likely or about as likely" and a risk model was used to calculate the objective risk (Waters et al., 2011). People can also be considered to be unrealistically optimistic if they predict that a future outcome for themselves will be more positive than that pointed to by an objective standard; this is what's known as unrealistic absolute optimism (Shepperd et al., 2015). This can be operationalised in a few ways. For example, some studies compare individuals perceived personal risk with population base rates. Others have compared predictions with actual outcomes (Shepperd et al., 2015).

There are some difficulties faced when determining the actual risk of the particular participants (Weinstein & Klein, 1996). For example, a woman may predict her risk of developing breast cancer to be lower than the average woman, indicating optimism. However, her individual risk may well be lower if her family history, alcohol consumption, age and other risk factors are taken into account. This can be dealt with by investigating comparative risk rather than absolute risk. A second problem in measuring the bias is that

individuals have been shown to have difficulty in understanding and postulating odds and risk probabilities (Yamagishi, 1997). Therefore, if people are estimating risks wrong, it could be because of an inability to understand the numbers (Weinstein & Klein, 1996).

There are many different causes of unrealistic optimism, with varying degrees of validity (Shepperd et al., 2002). Some explanations suggest that people are motivated to perceive their personal risks to be less than that of others around them because this is what they believe and want others to believe. Unrealistic optimism has potential benefits, for example, it can positively affect one's mental and physical wellbeing, and optimistic people have been shown to have a better quality of life (Conversano et al., 2010). Therefore, it is possible that these benefits drive unrealistic optimism. Within this explanation, researchers have hypothesised different explanatory accounts, such as a desire for self-enhancement, self-presentation or a belief that one is better than others when attempting to control the outcomes of a situation (Shepperd et al., 2002). Others have suggested that unrealistic optimism stems from different cognitive mechanisms that guide and influence how judgments are made. These cognitive mechanisms, or heuristics, could lead people to believe that their risk is lower than the risk of others. There are a few cognitive mechanisms that could do this. For example, the representativeness heuristic, where individuals estimate the likelihood of an event by comparing it to an existing prototype that already exists in the individual's mind (Tversky & Kahneman, 1981). A third explanation for the existence of the optimism bias suggests that people have an impoverished view of other persons compared to the vast amounts of information they have about themselves and that this informational difference leads to a divergence in risk estimations (Shepperd et al., 2002).

Both types of unrealistic optimism, absolute and comparative, have demonstrated behavioural consequences. For example, PMT suggests that people must perceive themselves as at risk from a certain threat if they are to undertake behaviours to deal with the threat (Prentice-Dunn & Rogers, 1986). Evidence supports this component of the theoretical model and shows that people are less likely to take precautionary actions if they perceive their risk towards a certain threat to be low (Floyd et al., 2000). The implication of this, then, is that optimism about one's risk can undermine preventative behaviours, which could lead individuals to take unnecessary risks (Shepperd et al., 2017).

As previously stated, the optimism bias has been demonstrated in the context of cyber security. Rhee et al. (2005), in a survey study on university students, found that for the four questions[1] that were used to measure perceptions of vulnerability, participants perceived that their own risk to cyber-security threats was considerably lower than that of the comparison targets. Therefore, demonstrating an optimistic bias in risk perceptions associated with cyber security (Rhee et al., 2005). These findings were further validated in a study in 2012 (Rhee et al., 2012). The 2012 study tested the same research on a sample of 204 MIS (management information systems) executives. The study found that the MIS executives perceived their own cyber-security risk to be significantly lower than the people they were being asked to compare themselves to. Therefore, this study demonstrates the optimism bias in cyber security beyond the student population. Furthermore, the study found that participants also demonstrated an illusion of controllability, suggesting that executives not only believe that they are less vulnerable than others to cyber-security risks but that they are also better able to control these cyber-security threats.

These two studies are just two examples of a reasonably established finding; the optimism bias is apparent in individuals' understandings of cyber security (Campbell et al., 2007; Chmielarz & Szumski, 2019; Cho et al., 2010; Haltinner et al., 2015; Kim et al., 2018). Studies have demonstrated great discrepancies between users' perceived and actual online threats. For example, Weinstein (2004), as cited in Campbell et al. (2007), in a study of 329 computer users, found that 77% of participants felt that their computers were safe from cyber security threats over the Internet. However, testing revealed that 80% of the participants' computers were infected with programmes that were tracking the participants' internet activities, and 19% of the computers were infected with computer viruses.

[1] In this study the participants rated their perceptions of risk related to their information system on a 7-point Likert scale from 'very low' to 'very high'. The same sets of questions were repeated to measure the participants' perceptions related to their friends' risk. These questions were: 1) The risk from information security threats to my system is; 2) The likelihood that my system is disrupted due to information security breaches in the next 12 months is; 3) The chance that my system will fall a victim to an information security breach is; and 4) The vulnerability of my system to information security threats is.

Other studies have demonstrated that the optimism bias can lead to poor security behaviours. Although individuals are often aware of cyber-security risks, such as online privacy risks, they still may be inclined to take risks because they are unrealistically optimistic (Chmielarz & Szumski, 2019). Furthermore, another study, using longitudinal methods, found that Cloud providers suffer from "unrealistic optimism" and subsequently underestimate their services' exposure to cyber-security risks (Loske et al., 2013). This, in turn, reduces the propensity to implement necessary IT security measures in the Cloud (Loske et al., 2013). Therefore, the finding of the optimism bias within cyber security has important implications for research and practice. As has been demonstrated by the above studies and the previous section on the consequences of the optimism bias, this strong tendency to underestimate one's own risk may lead to a reduction in taking precautionary action (Rhee et al., 2012). However, most of these studies are largely survey-based, and qualitative research may shed more light on how these biases are constructed. Nevertheless, such studies set a precedent for other cognitive biases to be applied to cyber-security behaviours.

2.3.2 Fatalism

Fatalism is another cognitive bias that has been found to influence perceptions and behaviours in regard to different risks. In this context, fatalism refers to an outlook where risks are controlled by external forces and a view that individuals are powerless to change this (Niederdeppe & Levy, 2007), or whereby an individual or individuals passively deny personal control of a situation to an attitude of resignation in the face of events that are thought to be inevitable (Xie et al., 2019). This has led to the coining of the term and model of rational fatalism, whereby risks become rational if a person believes they have no control over the outcome. According to this attitude, people who are convinced that a bad outcome is certain to happen would perceive no benefit from reducing their risk-taking behaviours (Kerwin, 2012; Xie et al., 2019). This cognitive bias has been found to be prevalent in regard to health risks, such as cancer (Befort et al., 2013). Befort et al. (2013) found individuals to have fatalistic beliefs about cancer prevention, which was also influenced by other demographic factors, such as whether participants lived in urban or rural areas.

Evidence of fatalism has also been prevalent in a few studies related to cyber security (Lawson et al., 2016; Xie et al., 2019). This research has shown that people with fatalistic beliefs about technologies are less likely to protect their privacy on the Internet (Xie et al., 2019). Furthermore, returning to PMT and fear appeals, high levels of fear in the absence of clear efficacious information about how to respond to the threat has been shown to lead to a sense of fatalism (Lawson et al., 2016). Other research studies have also focussed on the idea of privacy fatalism, the idea that rights to privacy are dead or dying (Penney, 2019). The validity of these findings could be improved by qualitative research and research investigating the manifestation of fatalism in real-life settings. This highlights the importance of tackling fatalism and ensuring that awareness campaigns do not engender it.

2.4 Summary of Psychological Theory, Research and Biases

Overall, this section has described previous psychological theories and research and how they have been applied to the field of cyber security. It was demonstrated that of the three theories discussed, PMT has been studied most frequently in the area of cyber security and has therefore gained the greatest support (Haag et al., 2021). However, it has been more widely studied with quantitative research techniques. The components of TPB and the EPPM have also been found in cyber-security contexts, however, the main support for these two theories remains within other areas such as health research. The study underpinning this thesis, rather than provide additional relationship validation among the components specified by PMT's rigorous theoretical foundation, demonstrated both in other contexts and in a cyber-security context, employs these components by adopting qualitative research within an organisation. Moreover, the current study will analyse if the components of these theories can be used in conjunction with usable security research to provide insights. How the current research will apply such theories to the interpretation and discussion of research findings will be discussed in section 2.10 of this literature review. This section has further demonstrated how previous research on biases could be useful in the context of cyber security. There are of course, many more biases have been researched in psychology than the ones mentioned in the above sections, such as memory biases and health biases (Harvey,

2007; Masiero et al., 2018). However, the current research was motivated to focus on the optimism bias and fatalism in the literature review as they are the ones that have been empirically tested in the field of cyber security and because of the biases that emerged in the data. It should be noted that the findings around biases were not constrained by the literature as the current research took a ground-up approach to data analysis. This will be further discussed in the methods section of this research.

2.5 Usable Security

Usable security is a branch of HCI scholarship focussing on human-centred security and privacy (Renaud & Flowerday, 2017). One of the seminal pieces of literature in user-centred design, the design of everyday things (Norman, 2013), originally entitled the psychology of everyday things (Norman, 1988), looked at design in terms of user needs and used many psychological principles. Owing to such literature there has been an increase in focussing the design of technology around the user. Usable security focusses on advocating security that works for people rather than making people fit into preconceived ideas of security (Adams & Sasse, 1999; Furnell & Clarke, 2012; Zurko & Simon, 1996). The usability of systems and the needs of the users are considered a primary design goal in security system design cyber-security policy design (Adams & Sasse, 1999; Zurko & Simon, 1996). Much of this research has been based within organisations and has been very influential in the way industry, and academia sees the human in cyber security (Adams & Sasse, 1999; Nurse et al., 2011a; Sasse et al., 2001). Psychology has also been influential in usable security, with many of the key researchers and studies in the area stemming from psychology (Adams & Sasse, 1999).

The field emerged as a prominent area in the 1990s with the seminal paper 'Users are not the Enemy' (Adams & Sasse, 1999). The paper presented a study where it was found that users compromise computer security mechanisms, such as password authentication, both knowing and unknowingly. However, it was demonstrated that such behaviour was often caused by the way in which security mechanisms were implemented and users' lack of knowledge (Adams & Sasse, 1999). Based on these findings, the authors suggest that

security-focussed departments within organisations need to communicate more with users and adopt a user-centred design approach. This paper demonstrated a shift away from the previous narrative of HCI and cyber-security research, which had formerly focussed on the human as the problem (Goo et al., 2014; Hughes-Lartey et al., 2021; Lowry & Moody, 2015; Sabillon, 2022); attempting to remove the human from the process, or at least control the human element with strict compliance policies. However, it is important to note that there is still ongoing research, perhaps a majority of research, which takes the perspective of the human as the problem or 'weak link' in cyber security (Goo et al., 2014; Hughes-Lartey et al., 2021; Lowry & Moody, 2015; Sabillon, 2022).

Usable security can be understood as three 'waves' of research, as put forward by scholars Bødker (2006) and Renaud and Flowerday (2017). The foundation, or first wave, of research, focusses on individual factors. Within this wave, individual perceptions, cognitions and behaviours have been and continue to be, researched, tested and modelled. This research space encourages people to follow security rules and policies. Moreover, usable security scholars within this research space attempt to put forward a positive security notion (Renaud & Flowerday, 2017). The second wave of research focusses on more social and contextual factors, recognising that the individual did not stand alone in the security space. The third wave focusses on everyday security and meaning-making, along with the integration of technology into people's everyday lives (Renaud & Flowerday, 2017). Psychology and usable security are overlapping disciplines and are, in many ways, related concepts. Psychological research does not only look at the individual but also looks at social groups (Lindzey & Aronson, 1968), contexts (Pettigrew, 2018) and culture (Lehman et al., 2004). Therefore, the influence of psychology can be seen to some extent within all three waves of usable security research. Hence, a number of the papers discussed in the previous sections of this literature review would also be considered influential papers in usable security. As will be demonstrated, both usable security and psychology are important in the understanding of employees and organisations within cyber security.

For this literature review, based on categories described by Bødker (2006) and Renaud and Flowerday (2017), literature on usable security has been separated into these three described waves. However, it should be noted that other researchers have found other ways

to distinguish usable security literature using different dimensions. Moreover, in the current literature review, the studies' placement within the three waves was decided by the focus of the research. However, usable security is more complicated than this, with many papers including a variety of focus areas. For example, Blythe et al. (2015) looked at how individual and organisational factors influence security behaviours, meaning they could technically belong to wave one or two. In cases like this, a judgment call was made on the main focus of the research. The research is laid out in the subsequent subsections to tell a story of the field rather than put research into distinct categories. Therefore, despite the categories used for the review, usable security research co-exists and can be seen as interconnected. Therefore, the next section of this literature review will discuss previous research with the usable security 'waves', with a particular focus on research that applies to organisational cyber security.

2.5.1 The Individual as the Focus

Research within the first 'wave' of usable security attempts to understand why individuals behave in specific ways and how existing policies might constrain individuals or 'force' them into 'bad' behaviours. This research focusses on the individual capabilities of the human in the context of cyber security by investigating what works for individuals and what does not. The research generally finds that security systems, such as password policies, demand more time, effort, and attention than users can afford, especially given other job stressors they may be under (Benenson et al., 2015; Chua et al., 2017; Herley, 2013). The following paragraphs will demonstrate some of this research and point to any potential gaps in investigations.

Early work in usable security demonstrated how undesirable individual behaviour regarding passwords could be caused by the failure of policymakers to recognise individual aspects of 'human nature' such as unattainable or conflicting task demands, human memory, and lack of support, training and motivation (Renaud, 2011; Sasse et al., 2001; Sasse & Rashid, 2021). This can result in users making mistakes or sometimes using workarounds to cope with the volume of passwords (Beautement & Sasse, 2009). Since then, a plethora of research has

investigated and critiqued password policies. Such research generally concludes that users are, in general, concerned with maintaining security (Inglesant & Sasse, 2010), but existing security policies are too inflexible and difficult to match user capabilities (Beautement & Sasse, 2009; Inglesant & Sasse, 2010; Nurse et al., 2011b; Weirich & Sasse, 2001). Research also points to arbitrary markers of security, questioning the security of three log-in attempts (Brostoff & Sasse, 2003), password length (Shay et al., 2016) and password expiration (Habib et al., 2018). Therefore, password policies place demands on users that impact their productivity negatively and, ultimately, that of the organisations in which they work (Inglesant & Sasse, 2010; Kirlappos et al., 2013). Based on this, researchers suggest that organisations should consider usable security principles to increase overall security instead of focussing on maximising password strength and enforcing frequency and have suggested ways to improve policies, such as using adaptive passwords (Segreti et al., 2017). Password policies are additionally often studied as a singular aspect of security in isolation and not within the context of an organisation and other day-to-day security factors.

Aside from password management and policies, research in usable security has focussed on other usability issues within organisations. For example, Bartsch and Sasse (2012) found that the employees frequently reported that authorisation operation issues, such as restrictive policies, despite a high level of overall reported compliance, sometimes lead to circumvention of access control systems, such as sending documents via different means. This finding highlights another example of where policies can lead to 'bad' security behaviours. However, access control systems are more challenging to make usable than passwords. Usable security research has clear applications for password policies with clear researched solutions, such as password managers. However, access control to certain information and documentation is often regulated, making alternatives to strict policies less possible (Alwan, 2018).

Another area of usable security research looks at how individuals understand and approach the use of secure email (Ruoti et al., 2018). Research demonstrates that there are many usability trade-offs and that individuals do not understand security models (Ruoti et al., 2018). Research in the area of emails in this context has also primarily focussed on what is now known as 'phishing behaviours'. The focus in organisational research looks at individual

factors that might increase susceptibility to clicking on phishing emails and how susceptibility might be reduced. The research here overlaps with psychology-based research in this area. For example, Iuga et al. (2016) found that gender and the years of PC usage had a statistically significant impact on phishing detection rate in a web-based study. Furthermore, the psychological anchoring effect was also observed as participants tended to examine the first bit of the phishing link more than the end (Iuga et al., 2016). Other research has supported demographic influences, suggesting that women are more susceptible than men (Iuga et al., 2016; Sheng et al., 2010) and that the 18 to 25 age group is more susceptible than older age groups (Sheng et al., 2010). There is research to support the idea of younger generations experiencing more security issues. However, age differs depending on the study (Oliveira et al., 2017; Sheng et al., 2010). Research more specifically related to organisations further looks at what factors in a phishing email increase the likeliness of employees to click on them. Studies demonstrate that authority cues and urgency techniques also increase the likelihood of falling victim (Williams, Hinds & Joinson, 2018). The degree to which an email contains targeting factors has also been shown to have an impact (Flores et al., 2014).

Researchers have developed metrics to measure and train employees to spot phishing emails. The most popular of these methods is phishing simulations, whereby employees are sent fake phishing emails to teach them how to spot such emails. Reinheimer et al. (2020) also researched how to best train employees to spot phishing emails and when to best remind them within an organisation. It was recommended that six months would be effective. However, many of these methods have been criticised by the usable security and psychology-based literature (Kirlappos & Sasse, 2011; Kumaraguru et al., 2010). It is argued that the popularity of phishing simulations stems from their ease of use and their ability to give clear metrics rather than the efficaciousness of the method and their ethics (Kumaraguru et al., 2009; Kumaraguru et al., 2007; Sheng et al., 2010). These simulations may also reduce trust by making it seem to employees that their organisation is tricking them. Alternatively, such simulations may make participants reluctant to click on links, reducing their motivation to report real phishing emails. However, the ideas surrounding trust are essentially prospective at the current time, with little or no research asking employees how they feel and think about phishing simulations within their organisation.

The exploration of mental models in cyber security is also related to usable security. This concept has been borrowed from cognitive psychology and cognitive science (Gentner & Stevens, 2014). Mental models refer to internal models that individuals use to reason about the world (Blythe & Camp, 2012). Researchers in the field of cyber security have sought to understand mental models to improve communication with users and education about cyber security and security interfaces (Baig et al., 2021; Mohamed et al., 2017). Moreover, it has been argued that poor usability may contribute to the development of inaccurate mental models, which may reduce individuals' abilities to make informed security decisions (Williams et al., 2016). Some studies have found that individuals who have more articulated technical models perceive more privacy threats (Kang et al., 2015). Human-centred security researchers argue that if we understand the end-user and their comprehension of security better, we will be able to design security solutions and interactions more effectively (Volkamer & Renaud, 2013). In this way, the mental model research aims to better understand users and further support individuals in making well-informed security decisions (Nurse, 2013).

2.5.2 Social Mechanisms as a Focus

The research on individual factors discussed in the previous section remains important and ongoing. However, the second wave of usable security research focusses on social mechanisms in usable security. This research signifies a move from focusing solely on the individual to encompassing broader social behaviours and interactions within workplaces and with others (McSweeney et al., 1999).

Within organisations, research has looked at hierarchal and peer influences and the context of culture and industry. For example, Hu et al. (2012) found that top-management participation in cyber-security risk campaigns strongly influences organisational attitude towards compliance with cyber-security policies. Moreover, in addition to normative beliefs and self-efficacy, Flores and Ekstedt (2016) demonstrated that transformational leadership and security culture were strongly associated with stronger attitudes towards resisting social engineering. Further research demonstrates that trust in one's employees positively

influences managers' ability to have good leadership concerning cyber-security compliance (Paliszkiewicz, 2019).

Other research has pointed to the influence of peers and colleagues on cyber-security behaviour, some of which may lead to the development of cyber-security champions: employees within organisations who serve as cyber-security role models and mentors (Becker et al., 2017; Gabriel & Furnell, 2011). For example, one study found that those that were provided with peer feedback created stronger passwords when compared to those that were not (Dupuis & Khan, 2018). However, researchers argue that such champions should not be there to represent current cyber-security policies that do not work for users. Instead, champion programmes should seek to represent user needs by identifying where policies cause friction, are ambiguous or do not apply (Becker et al., 2017).

Research in this space has also looked at the idea of shadow security, whereby employees in organisations create workarounds (such as remembering passwords by writing them down) that are usually not visible to official security and higher management (Kirlappos et al., 2014). These workarounds generally reflect the best compromise employees can find between getting the job done practically and managing the risks to a standard they believe is 'good enough' (Kirlappos et al., 2015). Therefore, these workaround behaviours might not be as secure as the official policy would be theoretically. However, they work better in practice as employees do not feel they are sacrificing productivity. Research here suggests that this provides a basis for workable security, security solutions that fit the people and the business, and that organisations should learn from these behaviours rather than attempting to get rid of them (Kirlappos et al., 2014). Research has supported this idea and found that in two case studies with 200 interviews and 2000 surveys, employees adapt existing security processes and employ self-devised solutions when they consider security policies to impact productivity deemed unacceptable to them (Kirlappos, 2016). However, this may not be appropriate in certain industries where specific policies may be mandated by law. In such cases, it is argued that organisations should communicate that cyber-security policy is due to a set of security standards (for example, it might be necessary to have reliable audit trails of access to confidential data) and not because of mistrusting employees (D'Arcy et al., 2014).

Usable security researchers have also played a significant part in research surrounding the understanding of cyber-security culture, how it is collectively agreed upon, how it changes depending on organisation and geography, how it functions within organisations and how it influences attitudes and behaviours (Bada et al., 2019; Uchendu et al., 2020). It is argued that environment, context, and social norms surrounding the process of developing and implementing security are also crucial to the effective operation of the product or policy. For example, Flechais et al. (2005) found that trust in secure systems can influence an organisation's cyber-security culture and performance. The authors argued that in some cases, existing trust relationships within an organisation might lead to employees breaking security policies and practices. In fact, sometimes adhering to existing security policies can undermine social relationships within a group of peers by going against social norms (Sasse & Flechais, 2005). However, this research will be discussed in detail in section 2.7 of the chapter, which focusses on organisational research on cyber-security awareness training, cyber-security culture, and organisational case studies.

2.5.3 Everyday Security

Most recently, usable security research has begun to consider the 'everyday'. This 'wave' incorporates studies of the integration of technology into people's everyday lives, with broader use contexts and applications in comparison to other waves (Bødker, 2015). This includes exploring user experience and non-expert conceptions of cyber security; the mundane and routine experiences of people (Coles-Kemp & Jensen, 2019) as well as collective experiences (Albrecht et al., 2021) and meaning-making (Bødker, 2015; McCarthy & Wright, 2004). This 'wave' of research is also important for organisational studies, as 'everyday' security highlights that scholars cannot merely study experts in the field, and research needs to explore how security perceptions manifest in individuals in the context of their everyday lives, both inside and outside of work. In this way, understanding security as lived by people is seen as critical to improving security (Dekker & Faber, 2008). Coles-Kemp and Hansen (2017, p. 1) argue that 'everyday security is a form of sociotechnical security co-constituted of both technological protection mechanisms designed to protect assets and of relational social practices that enable people to build and maintain trust in their daily

interactions.' While this research has primarily been outside organisations, it also calls for the possibility of more everyday security research concerning organisations and workspaces, especially when we consider the new normal of remote working.

Such research includes Molotch's (2013) ethnographic studies of public sites such as the New York subway system. This study found that workers' routines fit or do not fit into official security policies dictated to the public, demonstrating that such policies do not always consider the day to day lived experiences of people who often prioritise efficiency and pleasure over security. Similarly, in their study of the current designs of cyber-security architectures, Ashenden et al. (2018) argue that within the current designs of such architectures, there is a lack of consensus as to whose security is being addressed. They argue that there is often a tendency for the state to focus on the security of technology rather than the security of the citizen. This argument has clear applications to organisational research where policies are often made to benefit law and audits as well as technology instead of individuals within the organisation itself.

Dourish et al. (2004), through a qualitative analysis of two different organisations, looked at how end-users went about managing security as an everyday, practical problem. It was found that much like other research suggests in usable security, when using technology, security was one of a range of considerations that encroach upon the practical accomplishment of work. The researchers, therefore, argue that security decisions arise in the context of a range of physical, social, organisational, and practical considerations and must be studied in reference to such factors (Dourish et al., 2004). For example, for research conducted within the year 2020, some findings must be considered in the context of the pandemic, with an understanding that this may influence views on cyber security and feelings of security more generally (Furnell & Shah, 2020). Cyber-security perceptions and behaviour do not stand alone but rather exist within other contexts and factors, especially those related to risk. Research within this space is often designed to study certain facets of security, such as understanding password behaviour, which has been extremely important and necessary for the field. However, research also needs to take contextual and environmental considerations to look at security functioning as a whole within organisations.

2.5.4 Positive Security

Another central aspect of usable security is the aim to shift the dialogue from demonising the human as the weak link to viewing the human more positively (Sasse & Rashid, 2021). Usable security scholars argue that calling people the 'weak link' implicitly blames individuals for not being able to comply with policies (Sasse & Rashid, 2021), when, as this literature review has demonstrated, this is not always the case and is often counterproductive. Within an organisational context, this weak link viewpoint could lead employees to believe that they are not capable and reduce self-efficacy. The positive security narrative has arguably led to more literature and more dialogue arguing for the human to be seen as a capable and valuable part of cyber-security systems (Sasse & Rashid, 2021). This means that policymakers need to trust and engage users rather than trying to design the human out (Kirlappos & Sasse, 2014). Historically, and still, to this day, human factors and the user in cyber security have been treated as the weak link, meaning that employees within organisations are generally mistrusted (Goo et al., 2014; Hughes-Lartey, Li, Botchey & Qin, 2021; Lowry & Moody, 2015; Sabillon, 2022).

In addition to the previous research discussed that suggested policies and technology are often to blame for human error rather than the human, usable security researchers have also put forward a more direct discourse to support the move away from the idea of the human as the enemy (Parkin et al., 2010; Reinfelder et al., 2019; Sasse et al., 2001). In their paper 'Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security', Sasse et al. (2001) argued that simply blaming the user would not lead to more effective security systems and outlined a vision of a holistic design approach for effective security. A multitude of studies since then have shown that, far from being the weak link, the insecure actions of employees are often due to the lack of user-centred security in technology and policy rather than out of inattentiveness or ill will (Beautement et al., 2008; D'Arcy et al., 2014; Inglesant & Sasse, 2010; Renaud, 2011). However, research is yet to look at how this dialogue of the human as the weakest link manifests itself in practice in the context of an organisational case study and whether this dialogue is changing. Research needs to understand whether and why employees might see themselves as the

weakest link and whether this relates to perceptions of the human factor more generally, or if this is a mindset that security professionals influence or put forward.

However, this portrayal of tension between leading employees in security roles within organisations (such as security managers) and employees whose primary tasks do not involve security (the users) is not as straightforward. Reinfelder et al. (2019, p. 1) argue that 'security managers are not the enemy either'. Reinfelder et al.'s (2019) study showed that owing to the absence of organisational structures that include users in security development processes, security managers unintentionally obtain a negative view of users, which leads to strict and rigid security measures that users cannot influence. The authors argue that to break this cycle, where it is not just the users but all humans in the process who need support, security managers need organisational structures, methods and tools that facilitate systematic feedback from users (Reinfelder et al.,2019). Similar research has argued for the application of usable security beyond end users, adding another human element for the discipline to consider (Acar et al., 2016; Green & Smith, 2016). Research further finds that employees and managers have different attitudes toward cyber-security policy, and different factors motivate compliance between these two groups (Balozian et al., (2019). These findings demonstrate that not all individuals within organisations hold the same attitude (Beris et al., 2015), suggesting that different strategies may be needed to influence their behaviours.

2.6 Summary of Usable Security Research

The usable security section of the literature review grouped related research into three waves, as described by Bødker (2006) and Renaud and Flowerday (2017). It was demonstrated that research within the first 'wave' focusses on understanding the individual, with research looking at understanding how the usability of policies and technology might impact individuals and some criticisms of current features of cyber-security policies and training. The second 'wave' section looks at how usable security research moved to include a focus on social. Such research looked at the influence of individuals on one another. The third

wave of usable security research was further discussed, and it was demonstrated that this research focussed on everyday security and meaning-making. Despite the split of research into waves for the purpose of the literature review, it is important to note that the research should be viewed as overlapping, with each of the waves influencing each other and often occurring in parallel. Finally, the concept of positive security was discussed in terms of how this represented a shift in the dialogue of human factors research. The usable security scholarship will be used in the current research to explain and give insight into the findings. How the current research will apply the usable security field to the interpretation and discussion of research findings will be discussed in more detail in section 2.10 of the literature review.

2.7 Other Organisational Research

This section looks at cyber-security research that has been done in organisations, with specific reference to cyber-security awareness campaigns and cyber-security culture. Firstly, in section 2.7.1, evidence to support the use of awareness campaigns, including research on the most evidenced based methods, will be discussed. Secondly in section 2.7.2, research on cyber-security culture will be discussed. The research presented will both have psychological and usable security influence as well as HCI research more generally. Finally, section 2.7.3 will also look at how specific industries have been researched, particularly through the use of case studies given that this is the chosen method of the current research.

2.7.1 Cyber-Security Awareness Campaigns and Training

Cyber-security awareness campaigns aim to educate employees on cyber-security issues and encourage employees to behave securely (Engbers et al., 2005). Usable security researchers generally argue that awareness campaigns should catch people's attention and convince them that security measures are worth their time. Cyber-security training aims to assist people in acquiring skills, such as how to recognise a social-engineering attack or how to use

technology in a secure manner (Sasse & Rashid, 2021). There are many delivery methods in awareness campaigns and training methods. Firstly, physical and web-based posters are standard delivery methods (Abawajy, 2014). Web-based virtual training strategies (Barron, 1998) are also now prolific in this area. Research has demonstrated them to be effective in creating awareness of cyber-security strategies (Willems & Meinel, 2012). Phishing simulations are widely used in public and private sector organisations to promote better end-user email behaviour and gain metrics on phishing click-through rates. However, the evidence of the efficaciousness of this technique is under debate, as are the ethics underpinning this approach (Kirlappos & Sasse, 2011; Kumaraguru et al., 2009; Kumaraguru et al., 2007; Sheng et al., 2010). Game-based training has been shown to be effective for cyber-security awareness and training skills, seemingly providing engagement and entertainment and teaching cyber-security concepts and practices (Cone et al., 2007; Cone et al., 2006). Furthermore, companies use email to communicate with employees about certain risks (Cone et al., 2007).

As discussed previously, PMT has been a major influencing theory in the development of awareness and behaviour-change campaigns within cyber security (Briggs et al., 2017). More recently, another well-known technique for security awareness campaigns has been 'nudging' (Briggs et al., 2017). Nudge related research looks at how cues could be used to nudge or guide people towards a particular behaviour or action, rather than mandate or force specific behaviours, and often uses PMT-based concepts to do so. Therefore, this type of behaviour change method acknowledges the role the user plays in the security decision-making process (Coventry et al., 2014). Nudges in this context generally refer to features engineered into digital environments to indirectly encourage good cyber habits, for example a message saying that an email came from outside an organisation. In one experiment of over 2000 people in 5 different countries, van Bavel et al. (2019) explored the effect of notifications inspired by PMT on security behaviour. It was found that coping messages inspired behaviour change more than threat appeal messages, but that both forms of nudging were influential in changing behaviour. The beneficial impacts of nudging on cyber-security behaviours have been supported more widely in the literature (Turland et al., 2015). However, enthusiasm for the use of nudges has not been unanimous, with academic- and industry-based sceptics questioning the ethics of this approach to an individual's autonomy,

especially when used by governments (Goodwin, 2012; Renaud & Zimmermann, 2018). This is because 'nudges' influence choice, usually without the awareness of the persons.

Blythe et al. (2020) also looked at how organisations used sanctions and rewards to motivate behaviour within awareness campaigns and training, specifically phishing campaigns. It was argued that sanctions, such as naming and shaming or notifying someone's manager, are problematic methods when attempting to reduce risky behaviours as they may reduce employee trust in the organisation as well as reduce productivity. It was found that in 90% of the organisations studied, sanctions were used. The authors argued that industry needs to take a more informed approach when using behaviour change strategies (Blythe et al., 2020). In a study of a higher education institution, Chen et al. (2018) further found that an employee's choice of complying with the organisation's cyber-security policy is based mainly not on formal sanctions but on informal sanctions and personal capability (efficacy). Such research highlights a constant problem in cyber security; that industry is often behind academic research, is not aware of the research, or does not use it, making new concepts increasingly challenging to study in natural environments (Blythe et al., 2020; Chen et al., 2018). Campaigns need to be considered, both in research and in industry, in the organisational structure in which they are implemented and the security awareness professionals driving such initiatives (Blythe et al., 2020).

Some research has looked at the design and implementation of cyber-security awareness campaigns based on academic studies. Bada and Nurse (2019) researched and proposed a high-level programme for cyber-security education and awareness for small-medium sized business enterprises (SMEs). The programme was based on evidence and included five main aspects: engaging with SMEs, improving security practices and culture, maintaining and updating resources for the programme, creating lists of trusted third-party resources, and communication strategies. Although this research is primarily for the use of SMEs, it demonstrates that awareness campaigns can be evidence-based and the usefulness of tailoring campaigns to specific sectors and organisations. There is still much research to be done on understanding current campaigns, how they are best implemented and how long-term behaviour change is best accomplished.

Broadly, some awareness campaigns in organisations are effective in creating information-security awareness (Talib et al., 2010). This has depended largely on the different persuasive techniques used and the context in which the campaign has been situated. For example, Hu et al. (2012) found that top-management participation in and support for cyber-security risk campaigns strongly influences organisational attitude towards compliance with cyber-security policies. Similarly, Ashenden and Sasse (2013) found that CISOs need to reflect and work on effective ways of achieving credibility in their organisations and work on communicating with employees and engaging them in security initiatives from the top down. However, Da Silva and Jensen (2022) find that CISOs hold a great position of power within organisations, where their role is not only to interpret cyber-security information but to relay this to senior management. Other research suggests that cyber-security campaigns benefit from getting users to think proactively about security rather than being rote and requiring only passive listening (Cone et al., 2006). Investigations have further found that combined delivery methods are better than one individual security awareness delivery method (Abawajy, 2014).

Despite the popularity of cyber-security awareness campaigns to communicate risk to and change the cyber-security behaviours of employees and the demonstrated success of some of these campaigns and their techniques (Cone et al., 2006), they are not exempt from criticism in the literature (Bada & Sasse, 2014). Firstly, a company's aim is generally to make themselves more secure by communicating the risk of cyber-attacks to employees and thus creating awareness to change behaviour. However, creating awareness is not necessarily enough to drive behavioural change (Bada & Sasse, 2014). Employees additionally need to have their misconceptions challenged and explained (Kirlappos and Sasse, 2012) and must have understanding and motivation to change their behaviours (Bada and Sasse, 2014). Additionally, cyber-security awareness plans are limited to organisations, or departments within organisations, that do not have an existing awareness of cyber security. Many companies may indeed already have a high awareness of the company's issues and responsibilities surrounding cyber security.

Furthermore, users may not be motivated by campaigns to change their behaviours if they deem there to be a security-convenience trade-off that favours convenience (Tam et al.,

2010). For example, and as noted in relation to usable security, some password policies may be too demanding for employees and reduce employee productivity, leading to, despite knowledge and awareness of good password practice, employees going against organisational policy (Tam et al., 2010). Therefore, in a lot of cases, those employees using workarounds to bypass policies are not corrupt but are simply trying to do their work efficiently despite poor policies (Koppel et al., 2015). Therefore, when cyber-security campaigns suggest protective actions, they must ensure that employees can achieve these without impacting productivity.

Research has also demonstrated a link between cyber-security awareness campaigns and cyber-security culture. Wiley et al. (2020), in an online questionnaire study of 508 workers in Australia, explored the relationship between cyber-security awareness, organisational culture and security culture. The study results showed that while organisational culture and security culture correlated with cyber-security awareness, cyber-security culture played an important mediating relationship between organisational culture and cyber-security awareness. This highlights, again, the importance of context when looking at cyber-security awareness campaigns. Based on this finding, the authors suggest that organisations should focus on building a positive security culture in order to improve cyber-security awareness (Wiley et al., 2020). This leads us to the next section, which looks at the research surrounding the idea of cyber-security cultures within organisations.

2.7.2 Cyber-Security Culture

Over the last decade, there has been an increased interest in the concept of cyber-security culture, both in several different sectors of industry and the academic literature (Durojaiye et al., 2020; Uchendu et al., 2021). Cyber-security culture, also referred to as information-security culture and security culture within the literature, refers to an omnipresent set of assumptions, behaviours, norms, and values developed and shared by colleagues of an organisation towards different aspects of cyber security (D'Arcy & Greene, 2014; Ertan et al., 2020). In turn, this determines the mindset of employees towards cyber security within the organisation. Therefore, one's organisational cyber-security culture might include previously

discussed terms, such as shadow security behaviours. The concept, much like that of broad organisational culture, is contested, and so the definition changes between studies (Ertan et al., 2020). However, there seems to be a common understanding that it contains shared norms and values. Cyber-security culture is also part of a broader organisational culture, the most well-known and all-encompassing definition of which is 'how things are done in an organisation' (D'Arcy & Greene, 2014; Van Niekerk & Von Solms, 2010). Organisational and cyber-security cultures are likely to be different for each organisation, as they are dictated by many factors, such as whether people work individually or in teams or how closely people are managed (D'Arcy & Greene, 2014).

Within the literature, there is a dialogue regarding what is seen as a 'good' or 'positive' cyber-security culture and what is seen as a 'bad' or 'negative' cyber-security culture (Da Veiga & Martins, 2015; Glaspie & Karwowski, 2017; Ruighaver et al., 2007). Much of the work argues that a 'good' or 'positive' cyber-security culture includes employees who adhere to security policies, high levels of employee reporting, employees who feel comfortable reporting, and where security is a priority across all levels of an organisation (Glaspie & Karwowski, 2017; Ruighaver et al., 2007). A 'bad' or 'negative' cyber-security culture then may encompass a lack of understanding of cyber security, a demotivated attitude towards cyber security, and a lack of compliance with security measures. However, usable security scholars point out that organisations cannot expect to have a cyber-security culture that they deem as 'good' without there being usable policies and without listening to what works for users. 'Good', it is argued, should not be an unattainable standard. In organisations where genuine security needs underlie such behaviour and where a positive security culture is in place, compliance can become a shared value and a source of pride (Sasse & Rashid, 2021).

The idea of employees making cyber security a key responsibility is also visible in the literature as a path to a better cyber-security culture, often through better compliance (Kim & Han, 2019). Some research shows that increased levels of responsibility in employees lead to increased levels of compliance (Kim & Han, 2019). This research has led to the creation of training methods that aim to increase responsibility, such as through games (Filipczuk et al., 2019). Using games as training methods is suggested to increase engagement with, and therefore knowledge of, the content of the training. Other research demonstrates that

individuals devolve responsibility for their cyber security to technical interventions and senior management (Tischer et al., 2016). Research suggests that many individuals do not feel they have the skills to fulfil a cyber-security responsibility (Hadlington, 2018). Research shows that security professionals and non-security related employees may have different ideas surrounding responsibility (Posey et al., 2014). However, there is debate in the literature as to what extent responsibility should be put on employees, especially when employees need to focus on their primary work, which may be vital, such as in healthcare. Many organisations, especially large global businesses, have specific cyber-security teams. Therefore, it can be argued that these teams need to take the main responsibility while trusting employees to act responsibly.

Within each cyber-security culture, it is important to note that subcultures can arise (Da Veiga, 2016; Da Veiga & Martins, 2017; Hofstede, 1998; Kolkowska, 2011; Muendo, 2014; Whelan, 2017). For example, some research has pointed to differences between managers and users regarding security behaviours. Albrechtsen and Hovden (2009) found a digital divide between users and managers; cyber-security professionals primarily regarded users as a cyber-security threat, whereas users believed themselves to be an untapped resource for security work. Moreover, Balozian et al. (2019) found that different levels of users within organisations are affected by different techniques that encourage cyber-security behaviours. Similarly, research has demonstrated that cyber-security culture may differ by office location and between those in IT roles and non-IT roles (Da Veiga & Martins, 2015). This suggests that there is no one-size-fits-all model for understanding an organisation's behaviour and culture.

A few large literature- and systematic- reviews have sought to appraise previous research on cyber-security culture. These reviews look at what factors have been found to impact cyber-security culture, the methods used to look at culture, and how and where such methods have been applied most effectively. Karlsson et al. (2015) conducted a literature review on cyber-security culture research published between 2000 and 2013. Findings showed that the topics most researched were those looking at the relationship between culture/organisational culture and cyber security and frameworks for cultivating a cyber-security culture. The researchers further concluded that the majority of the research found was descriptive, philosophical or theoretical and lacking in a structured use of empirical data. The researchers

suggested that future research should study the identified research topics in greater depth; focus more on creating theories or testing theories to increase the maturity of the field; and use a broader range of research methods (Karlsson et al., 2015).

More recently, Uchendu et al. (2021) conducted a systematic review of the previous 10 years of research regarding cyber-security culture, which identified 58 research articles. The review highlighted several key findings. Firstly, the review showed that top management support, security policy and cyber-security awareness and training were the key factors shown to be most influential when organisations build and develop cyber-security cultures. Moreover, developing a security culture requires in-depth knowledge of the given organisation and its employees. Questionnaires and surveys were the methods most often used to measure culture. Furthermore, very few approaches have been evaluated in real-world environments (Uchendu et al., 2021). The review also looked at what sectors had been researched. It was found that there were three articles focused on healthcare, two on banking and finance, one on retail, and six on public organisations. The other selected papers did not focus on a specific industry. Finally, the researchers argue that in the future, it would be ideal for academics and industry practitioners to work closer together on research looking at cyber-security culture (Uchendu et al., 2021). Without research within organisations, it is difficult to ascertain the actual value of previous research and whether it might impact real-world cyber-security culture. If practitioners and academic researchers co-operate, it will enable researchers to access real organisations to apply, evaluate and refine their new research. Furthermore, those in industry will gain access to research expertise, which is often inaccessible. This would, after research has been widely investigated, ultimately lead to the design and development of a robust set of approaches suitable for those organisations to use (Uchendu et al., 2021).

2.7.3 Organisational Research Methods

The research methods in human factors research in the field of cyber security are still arguably heavily quantitative, survey-based, or experiment-based (Iuga et al., 2016; Flores et al., 2014; Kirlappos & Sasse, 2011; Renaud, 2011; Sheng et al., 2010; Vance et al., 2012).

Though methods used for research in usable security have perhaps been more qualitative than research directly from a psychological point of view (Blythe et al., 2015; Flores et al., 2014; Kirlappos et al., 2013; Reinheimer et al., 2020). However, a lot of the literature is not empirically based but uses previous research, real-world examples or opinions to forward the area (Bada & Nurse, 2019; Renaud, 2011). While such methods remain extremely useful, they may be supplemented with deep insights from qualitative work within broader contexts.

Research on cyber-security culture has been particularly quantitively based. Researchers and industry professionals have developed many survey-based instruments to investigate organisations' cyber-security cultures. These are usually quantitative, with few studies using any qualitative methods (Sas et al., 2021). Such methods have significant value (Da Veiga & Eloff, 2010; Rantos et al., 2012). However, they present an issue for organisations (Uchendu et al., 2021). For example, many of these questionnaires ask knowledge-based questions, which do not necessarily influence behaviour and participants in such surveys can be influenced by priming and question structuring (Krol et al., 2016). Surveys also look for broad cultural meaning in organisations and do not necessarily best reflect nuanced cultural differences between groups within a single organisation. Additionally, surveys are often just a snapshot of cyber-security culture and do not look at longitudinal aspects of culture (Uchendu et al., 2021). Researchers also assert that it is important for cultures to be understood in their organisational environments and within threat landscapes, or at least employee understandings of threat landscapes. Therefore, organisations using survey tools need to conduct them regularly, raising the argument for more dynamic measurements and understandings. Currently, literature reviews demonstrate that future research needs to evaluate culture, or models, in-situ (Uchendu et al., 2021).

Case studies have been a valuable research method when investigating cyber-security concepts within organisations (Karlsson et al., 2015). However, they are far from the most used method, with even fewer studies using qualitative methods and in-depth investigations of a single organisation or sector (Uchendu et al., 2021). No research studies were discovered at the time of writing that aim to take a holistic approach to understanding everyday security behaviours, perceptions, and cultural aspects within a single organisation using psychology and usable security literature.

As discussed above, many current case studies have focused on purely understanding cyber-security culture (Da Veiga & Martins, 2015; Nasir et al., 2019; Tang et al., 2016). These studies have been useful in understanding the relationship between culture and compliance, managerial insights and testing models seeking to measure compliance and cultural factors. Outside a focus on organisational culture, one case study also sought to investigate organisational attempts to provide usable security products across three firms (all providers of cyber-security systems), some federal and some private. It was found that the adoption of usable security was usually motivated by employee and customer complaints (Caputo et al., 2016). A few other case studies have focussed on understanding cyber-security challenges within the healthcare domain (Ghafur et al., 2019) and higher education institutions (Durojaiye et al., 2020). All of these case studies show the value of this method.

2.8 Where are we now?

Thus far, this literature review has aimed to summarise the previous research from psychology, usable security and wider HCI research seeking to understand the cyber security of employees within organisations, as well as demonstrate the need for more research in certain areas of these bodies of scholarship. The literature review has shown that psychology and usable security, fields which have overlapped and influenced each other, have greatly helped a broader understanding of the human element of cyber security within organisations. However, certain viewpoints, such as positive security and methods such as case studies, have been underused compared to questionnaires and surveys (Uchendu et al., 2021). Researchers argue that human-centred security and privacy research still lacks maturity in many ways (Renaud & Flowerday, 2017). Firstly, many security products remain low in usability standards. Secondly, most of the cyber-security industry relies primarily on awareness-raising and training endeavours to improve their employee and organisational resilience to cyber-attacks and general cyber-security issues. Nevertheless, the number of successful hacking attacks increases each year, so there is perhaps little evidence that current awareness-raising methods are particularly effective (Renaud & Flowerday, 2017).

The research reflects a need for more 'positive' security research and dialogue, both within academia and industry (Zimmermann & Renaud, 2019). The viewpoint that the 'human is the weakest link' is still arguably the most prominent view within industry and research (Goo et al., 2014; Hughes-Lartey et al., 2021; Lowry & Moody, 2015; Sabillon, 2022). This is despite the plethora of research over the last few decades demonstrating that the 'human as the weakest link' discourse is not only unhelpful but largely invalid (Beautement & Sasse, 2009; Inglesant & Sasse, 2010; Nurse et al., 2011b; Weirich & Sasse, 2001). For example, decades of research has demonstrated the importance of efficacy in cyber-security behaviour, among many other important factors. Zimmermann and Renaud (2019) similarly argue that the assumption that the human constitutes a problem to control is deep-rooted, giving examples of where employees have been blamed for cyber-attacks despite employee behaviour not triggering the given breaches. If underlying assumptions of employees are unfounded or wrong, then the solutions developed will also be ineffective or mismatched. Currently, therefore, employees are excluded, trained, constrained, and controlled to comply with security policies (Zimmermann and Renaud, 2019; Weirich & Sasse, 2001). Therefore, Zimmermann and Renaud (2019) argue that there needs to be a complete paradigm shift that recognises the employee as a contributor to success within wider socio-technical systems. The research, therefore, needs to be conducted to understand the current cyber-security views of employees. Furthermore, for this to happen, more open-source collaborative research between academia and industry needs to take place (Uchendu et al., 2021). This will allow academics to see if previous research holds within context and to what degree, as well as give industry experts a chance to understand such perspectives and apply them.

Additionally, as highlighted in many of the studies and analyses in the previous sections, specific research methods need to be used to get deeper insight from different and more multidimensional perspectives. Researchers in the field suggest that there is still an ongoing focus on technical aspects of cyber security due to a lack of consolidation of the attributes pertaining to human factors, the application of theoretical frameworks, and a lack of in-depth qualitative studies (Jeong et al., 2019). Therefore, Jeong et al. (2019) propose that future studies focus on: consolidating human factors, taking an interdisciplinary approach when examining cyber security, and conducting additional qualitative research whilst investigating

human factors in cyber security. The perspective that more qualitative research is needed for a mixed methods understanding of cyber security is echoed by other researchers in reference to multiple aspects of cyber-security research, such as cyber-security culture (Sas et al., 2021; Uchendu et al., 2021).

2.9 Impact of COVID-19 on Cyber Security

In early 2020, the Coronavirus (COVID-19) was declared a pandemic by the World Health Organisation (WHO, 2022). This global crisis has meant that millions of people have been forced into quarantine and social isolation as governments, to different degrees, imposed local and national `stay at home' orders. The pandemic also led to the largest number of employees globally being confined to lockdown measures and, by extension, required to work remotely (Ahmad, 2020), creating a number of challenges for workplaces. Employers had to ensure that their employees could move to a remote environment, not only quickly and safely concerning the pandemic but also securely, while employees had to establish new ways of working away from the workplace. At the same time, many researchers have argued that the cyber-security threat landscape went through a significant change. In this section, research looking at how the COVID-19 pandemic will be discussed in terms of how it has impacted the cyber-security landscape. Moreover, research looking at the impact of remote working, wellbeing and their impact on cyber security will be discussed.

2.9.1 The Changing Threat Landscape

Not only did the COVID-19 pandemic have a remarkable impact on society and the global workforce, but it also engendered a new wave of cybercrime-related circumstances. This, in turn, has implications for society, the workforce and researchers. Since the beginning of the outbreak, certain types of COVID-19 cyber-security incidents and attacks have been reported. For example, there were many scams where individuals impersonated public figures or authorities, particularly those related to public health (Chigada & Madzinga, 2021; Lallie et al., 2021; Muthuppalaniappan & Stevenson, 2021). These scams targeted both members of

the public and employees within organisations. Cyber-attacks also attempted to disrupt critical national infrastructure such as health care services (Lallie et al., 2021). Moreover, security risks began to emerge because of the realities of the COVID-19 period. For example, a lack of remote-working security awareness and training, heightened stress and anxiety among employees, new technologies, rushed technology deployment, and the presence of untrusted individuals in a remote-working environment, for example in flat shares (Nurse et al., 2021).

Lallie et al. (2021) conducted an analysis of cyber-attacks throughout the pandemic. The results of the analysis demonstrated that following initial gaps between the initial outbreak of the pandemic in China and the first pandemic/COVID-19 related cyber-attack, attacks began to become steadily more prevalent to the extent that at point 3 or 4 unique cyber-attacks were being reported daily (Lallie et al. 2021). This demonstrates how frequently cyber criminals began to utilise the pandemic for cyber-attacks. Supporting the findings of Lallie et al. (2021), Chigada and Madzinga (2021), in a systematic review of the literature from December 2019 to June 2020, found that there had been an exponential growth of cyberattacks and threats during the first few months of the pandemic. Moreover, Pranggono and Arabo (2021) studied the cyber security issues that occurred during the COVID-19 pandemic, emphasising a correlation between the ongoing pandemic and the increase in cyber-attacks targeting sectors that were/are vulnerable. Furthermore, the authors argue that the growth in anxiety and fear that stemmed from the pandemic increased the success rate of cyber-attacks. Georgescu (2021) further found that COVID-19 restrictions generated an increase in phishing and Remote Desktop Protocol (RDP) attacks and that both RDP and phishing attacks were the leading causes of an intensification of ransomware attacks. Moreover, the authors show that the pandemic also raised the issue of cyber security in relation to the new normal of expecting staff to work remotely, mainly from their own homes. Remote working increases the possibility of phishing and ransomware attacks, as well as those of a state-sponsored nature (Pranggono & Arabo, 2021). Other researchers and industry leaders have further highlighted threats to particular industries such as healthcare and the financial sector (Aldasoro et al., 2021).

2.9.2 Remote Working During COVID-19

The move to remote working, or working from home, was and is, at the time of writing, widespread during the pandemic. Some research has demonstrated that remote working has a positive impact on employees. A case study at IBM (Heinonen, 2009) demonstrated that flexible working increased perceptions of productivity. In this study, women, in particular, placed high importance on working from home as a positive benefit (Heinonen, 2009). Moreover, a research study conducted in China found that employees working from home reported improved work satisfaction, their attrition rates halved, and that working from home led to a performance increase of 13% (Bloom et al., 2015). However, this previous research on remote working can be questioned in a pandemic context (Wang et al., 2021). Previously, remote working could be seen as an option rather than mandated and was often part of flexible working strategies where employees would spend time in and out of the office. Research reports that in 2015 only around 2% of the European workforce worked mainly from home (Wang et al., 2021). Previously, therefore, employees and their organisations had very little experience of mass remote working, which would seemingly impact their remote working experiences; allowing a few employees to work from home is very different from going from an entire workforce working in the office to working remotely almost entirely overnight.

Research in the current pandemic period has demonstrated that there have been both positives and challenges associated with this 'new normal' working context. Wang et al. (2021) found that some of the negatives experienced by those working at home during the pandemic were experiences of procrastination, ineffective communication, work-home interference, and loneliness. Similarly, Etheridge et al. (2020) reported that employees experienced productivity decreases, which were associated with decreased wellbeing. Research suggests that working from home in this context leads to an 'always on' mode, leading to mental and physical fatigue. Mustajab et al. (2020) further demonstrated that remote working could reduce productivity for reasons such as multitasking, childcare responsibilities, decreased motivation, and psychological issues. It has also been suggested that while there are no clear links between job satisfaction and remote working, remote working negatively impacts the work-life balance (Bellmann & Hübler, 2020). It is also

possible that the situational and behavioural consequences of remote working impact the cyber security of an organisation owing to changing employee priorities. However, it should also be noted that it is hard to tease out the difference between issues caused by the pandemic and issues caused by remote working.

To cope with the changing environments, organisations and employees now heavily rely upon video conferencing technologies to ensure the smooth running of teams, for example. These technologies have also impacted how we work, and research demonstrates they also impact workplace productivity and wellbeing. Waizenegger et al. (2020) interviewed 29 participants regarding their experiences of working from home. The participants reported reduced feelings of isolation when video conference meetings were held at the beginning of the day. However, participants also reported 'virtual meeting fatigue' or 'Zoom fatigue'. Further research demonstrates, from 10,591 participants, that hyper gaze from a grid of staring faces and the cognitive load from producing and interpreting nonverbal cues might contribute to 'Zoom fatigue' (Fauville et al., 2021).

2.9.3 Impact of Remote Working on Cyber Security

Remote working is by no means a new concept. However, it has never been so widespread, and arguably, prior to the pandemic, is not a context where cyber security has been a priority (Furnell & Shah, 2020). The increased reliance on technology for connecting people, and thus also employees, and the move to a perhaps 'less' secure home environment, remote working has had a significant impact on the cyber security of organisations and of employees (Khan et al., 2020; Lallie et al., 2021). Opportunistic cyber criminals pick people with specific vulnerabilities to take advantage of certain circumstances. This is nothing new; a natural disaster or ongoing public crisis allows attackers to take advantage of vulnerable people in a vulnerable situation. For example, in the wake of Hurricane Katrina, many fraudulent websites appeared appealing for humanitarian aid (Lallie et al., 2021). Studies on cyber security have focused predominantly on threats to cyber security, which have been argued to have been adapted to the new work or increased in the wake of the COVID-19 pandemic. These include but are not limited to an increase in Distributed Denial of Services (DDoS)

attacks and malicious domains using words such as ‘corona-virus’ and malicious websites. The spreading of Malware, Spywares, and Trojans, launching ransomware attacks and sending out spam emails relating to COVID-19. Furthermore, attackers are sending out malicious messages via fake COVID-19 information apps. Attackers are also using business email compromise scams by using coronavirus disease as a tool (Khan et al., 2020). A study from The Research Institute for Sociotechnical Cyber Security (RISCS) found that participants viewed inadequate remote working security controls or mitigations and decreased visibility of remote working environments to lead to more opportunities for employees to, deliberately or unwittingly, expose organisations to risk (Crossland & Ertan, 2021). Furthermore, the participants in this study argued that the risk of insider threats was higher during the pandemic owing to the remote working environment and having to on- and off-board employees remotely.

Therefore, the focus has also been on the need to adapt cyber-security awareness campaigns to the new working environment, not just in the way they are delivered but also in content. Previous research conducted prior to the pandemic suggests that cyber-security awareness is different in a remote environment (Johnston et al., 2000; Johnston et al., 2010). One study showed that, compared to their in-office counterparts, remote employees faced lower levels of vicarious experiences, verbal persuasion, and situational support (Johnston et al., 2000). This is argued to result in diminished levels of cyber-security policy awareness (Johnston et al., 2000). Later research conducted by the same authors further suggests that the lack of supportive materials, in verbal, demonstrative, or resource-based form, significantly disadvantages remote employees’ awareness of security and privacy policies within their organisations, reducing their compliance to these.

Other research has found that organisations took different approaches to security risk management (Crossland & Ertan, 2021). Some organisations relaxed corporate device policy and displayed increased trust in employees with cyber security, whereas others increased restrictions, occasionally to the perceived detriment of productivity and collaboration. This study further found that remote working increased worry about insider threats. Participants suggested that there were opportunities for employees to, likely unwittingly, expose organisations to risk (Crossland & Ertan, 2021).

Concerns have also been raised over the security of technology used to support the remote working environment. One of the most notable examples during the COVID-19 pandemic was the issues that arose relating to the security of Zoom (Furnell & Shah, 2020; Wakefield, 2020; Weil & Murugesan, 2020). Zoom, a software initially praised for its ease of use for team collaboration, was criticised for a range of privacy breaches, including false claims of end-to-end encryption and a security flaw that left some users vulnerable to having webcams, the ability for uninvited guests to join meetings and microphones hijacked (Wakefield, 2020; Weil & Murugesan, 2020). The chief executive of Zoom noted how the company had gained users on an unprecedented scale in an extremely short period of time (Wakefield, 2020). Updates were made quickly to fix these issues; however, it remains an example of how the sudden move to remote working could lead to unforeseen security concerns for home workers (Furnell & Shah, 2020). On the other hand, while not a welcomed situation, COVID-19 provided a catalyst for the provision of technology-based services to aid remote working. Whatever the changes, it can be seen that the current research did not take place in what could usually be considered a 'normal' cyber-security landscape.

2.9.4 Impact of COVID-19 on Cyber-Security Behaviours and Perceptions

Research into cyber-security behaviours, perceptions and awareness campaigns during the COVID-19 pandemic are thus far limited. One survey study evaluated the cyber-security culture readiness of organisations from different countries during the pandemic (Georgiadou et al., 2021). Results demonstrated significant variations among individual participants and organisations. 53% of the participants reported that they did not receive any security guidelines from their employers regarding remote working during this crisis (Georgiadou et al., 2021). Employees may also have not had the opportunity, especially if they were new to an organisation, to be properly trained in cyber-security behaviours before being moved to a home working office (Nurse et al., 2021). Moreover, this could have been exacerbated by reduced access to information/knowledge about security practices. For example, people may have more difficulty in quickly speaking with a work colleague about appropriate security behaviours when working from home compared to in the office (Nurse et al., 2021). The

impact of the context of the stress and pressure of the pandemic needs to be considered in relation to how the workforce views cyber security. At the time of writing, there is no literature looking directly at this issue. However, the impact of the pandemic, paired with the research discussed in the literature review, demonstrates the increase or change in cyber-security threats while working from home.

In addition to directly impacting individuals' cyber-security perceptions and behaviours, the COVID-19 pandemic has impacted society and the global workforce in various ways. Firstly, many people suffered from COVID-19 themselves. At the time of writing, 165,069,258 cases have been recorded worldwide (World Health Organisation, 2021). Many people have had to take care of sick family members or isolate themselves due to potential symptoms. Therefore, a crisis of this scope has many implications that impact research, especially that of a behavioural nature (Reynolds et al., 2008; Sim et al., 2004; Styra et al., 2008).

Emerging research conducted during COVID-19 demonstrates the pandemic's impact on the wellbeing of the global workforce (Unadkat & Farquhar, 2020). Zacher and Rudolph (2021) showed that, on average, life satisfaction and positive affect decreased between March and May 2020 in participants in Germany. Other research shows that levels of loneliness during the first stages of lockdown were high (Groarke et al., 2020). The UK COVID-19 Mental Health & Wellbeing study, a quota survey taken between 31 March 2020 and 11 May 2020, found that suicidal ideation increased over time, especially in young adults. However, the survey also reported that positive wellbeing also increased. The findings of all these studies demonstrate that the COVID-19 pandemic represents not only a major medical and economic crisis but a psychological one, as it can be associated with declines in people's wellbeing (Zacher & Rudolph, 2021). This research questions the extent to which people's security concerns would change, owing to the increase in other and arguably more pressing physical and mental health concerns.

It is important to note that wellbeing has been found to influence human actions and states considered important for functioning in the workplace. For example, tiredness, a side-effect of many mental health issues, has been found to lead to safety risks at work, often owing to slower decision making (Brown et al., 2020). Further research has demonstrated that those

with depression has a negative impact on interpersonal and workplace functioning (Katon, 2009). Moreover, the state of boredom has been demonstrated to increase financial risk taking (Miao, P., Li, X., & Xie, 2020). Research such as this demonstrates that certain physiological states and mental health conditions, such as those experienced during COVID-19, have the potential to impact individual job functioning, in which adherence and attention to cyber security policies could be included.

A study from (RISCS) found that positive organisational handling of employee wellbeing was reported when respondents felt leadership clearly articulated and justified a consistent approach to remote working (Crossland & Ertan, 2021). Many participants in this study did note wellbeing-related positives of remote working, such as spending more time with family and reduced commuting time. However, a few participants also expressed concern about impending transitions back to working from the office, which would likely have its own challenges as employees change routine once again, relating to both wellbeing and security practices. This demonstrates that events not directly related to cyber security may still influence cyber-security perceptions and behaviours.

2.10 Summary of Literature Review

This literature review aimed to discuss research and academic dialogue surrounding psychological and usable security-driven research on the human factor in cyber security within organisations. Firstly, the literature review described risk perception and behavioural change theories from psychology: Protection Motivation Theory, the Extended Parallel Process Model and The Theory of Planned Behaviour. Research on the application of these theories to the cyber-security literature within organisations was discussed and critiqued, as well as gaps were highlighted. As PMT and the constructs of other theories are proposed to lead to maladaptive coping responses, and given the research available, the review also looked at the optimism bias and fatalism and how these two cognitive thinking methods may impact cyber security. The similarities and differences, and two-way influence, of psychology and usable security were then described before the review went on to highlight usable

security research and literature. The three waves of usable security were demonstrated and analysed. Furthermore, the review highlighted previous human factor organisational research within cyber security, demonstrating where there were gaps in the literature. The review then concluded with an overview of where the human factors in the cyber-security field stand now, as well as a summary of the context of where we are now in terms of the pandemic and its influence on current research.

The concepts from PMT, the EPPM and the TPB, along with other psychologically-based research, will be used as analytical lenses to interpret and gain a deeper understanding of the current findings. Moreover, dialogue and previous research from the HCI and usable security field will be used alongside psychological theories and research as complementary analytical lenses that will assist in offering explanations and insights into participants' perceptions and behaviour. As will be discussed later in Chapter 3.7 the data analysis began with a thematic analysis from which several broad themes were identified. These themes were bought into conversation with the theories and research discussed in the literature review, assisting the researcher in identifying linkages between the data and previous research. In some cases, previous research assisted in identifying some of the themes and subthemes, for example, previous work on the optimism bias assisted in the discovery of this bias in the current research. This approach to understanding findings is well established in qualitative research within cyber security, where meaning and knowledge are developed through the application of existing theory to data (Burdon & Coles-Kemp, 2019; Da Silva, 2022).

Chapter 3. Methodology

3.1 Introduction

This research took a case-study approach to gain a deeper understanding of cyber-security behaviours in organisations through the lens of cognitive and social psychological theory and usable security research. The research aimed to understand cyber-security culture, perceptions, biases and behaviours in the context of a private global organisation and understand the potential similarities and differences between employees and groups of employees (such as differences between those who work in certain job roles) in this context. To meet the aims of this research, the thesis uses a qualitative case-study methodology within a single organisation, by using distinct methods, namely semi-structured interviews, elite interviews and focus groups. Firstly, Section 3.2 will examine the case-study approach in qualitative research, looking at both the benefits and drawbacks of this approach and why this method was chosen for this research. This section will also describe the organisation chosen for this study. In section 3.3 the impact and context of the COVID-19 pandemic will be discussed in terms of the effects on the research methodology, the organisational case study, and the participants. Section 3.4 will outline the specific research methods chosen to investigate this case study. These methods will be described and evaluated, as will their applicability to online video conferencing methods. In total, 42 participants took part in this research. The participants and their demographics will be described in section 3.5. Sections 3.5.2 and 3.5.3 will also look at the interview and focus group process, as well as the ethical considerations taken in this research. The data was analysed by means of a thematic analysis method using NVivo 12, a qualitative data analysis software. This process and the transcription process will be described in Section 3.6. This chapter will then look at the possible limitations of the research. This section will end with a description of the research journey, including previous research conducted by the researcher that inspired this case study.

3.2 Research Design: Case Study

3.2.1 The Choice to Use a Case Study

The case-study approach allows for in-depth, multi-faceted investigations of complex issues in their real-life settings (Crowe et al., 2011) to amplify an understanding of the said issue. This type of research is often praised for its descriptive accuracy (Wikfeldt, 2016). To conduct case studies is to attempt the creation of understanding and hypothesising rather than quantifiably stating statistical facts (Yin, 2012). The approach is, therefore, usually employed when there is a need to obtain a deep understanding of a topic. Case studies are often referred to as a "naturalistic" design, in contrast to an "experimental" design in which the researcher exerts control over and manipulates the variables of interest (Crowe et al., 2011). Broadly, the case-study method describes a way to codify observations (Cavaye, 1996). Furthermore, case-study research aims for an in-depth understanding of the context in which a phenomenon is being observed (Cavaye, 1996). It allows for the study of a wide variety of variables and different aspects of a given phenomenon. These variables do not have to have been predetermined.

The case-study method can be understood better as a research type that may encompass a range of approaches, such as content analysis, surveys, interviews and focus groups (Starman, 2013). Case studies may therefore encompass both qualitative and quantitative techniques (Seawright & Gerring, 2008). Case studies have long been used as a design method and have been especially valuable in practice-orientated fields, such as medicine, psychology, education, and management (Starman, 2013). It has, therefore, also been seen as a useful method for understanding the practicalities and workings of cyber security in organisational contexts (Ali et al., 2020; Antunes et al., 2021; Kuypers et al., 2016; Osborn & Simpson, 2017). Previous work demonstrates the usefulness of this method in understanding an array of cyber-security issues and phenomena. However, few of the case studies to date in the realm of cyber security aim to gain a deep understanding of the complexity of the human factor within an organisational context.

Some research has used the case-study approach to understand the uptake of different security systems and cyber-security management approaches (Ali et al., 2020; Antunes et al., 2021). Ali et al. (2020) studied the uptake of cloud computing and how cyber-security risks

were considered in the context of an Australian local government authority. This research adopted a mixed-methods approach to the case study, using both interviews and survey methods. Using these methods, the researchers were able to gain an understanding of the role of technical complexities in terms of data security towards cloud adoption as well as Identify new developments and challenges in cloud security requirements, such as risk mitigation practices (Ali et al., 2020). The authors argue that via the use of these research methods, they were able to increase scholarly insights into the security aspects of cloud computing within the local government sector and posit that the research provides critical insights for future governments adopting cloud services (Ali et al., 2020). Antunes et al. (2021) used a case study to understand the implementation of a cyber-security management project in SMEs. The methods allowed the authors to demonstrate the substantial benefits to the audited and intervened SMEs, largely related to their cyber-security management robustness and collaborators' cyber awareness. The case-study method used here allowed the researchers to gain a deep understanding of the design and implementation of a security management project, which might not otherwise have been understood through other means.

A few case studies have sought to understand and improve security culture through monitoring tools, implementation actions, and security awareness training (Chen et al., 2006; Da Veiga & Martins, 2015; Eminağaoğlu et al., 2009). Chen et al. (2006) used a case-study methodology to evaluate a cyber-security awareness system within an organisation. After deploying the cyber-security awareness system, the researchers interviewed users and managers to gain insight into the system's use. This allowed for a deep understanding of how the system was used as well as employee suggestions which could serve as guidelines for future systems. The findings of this study demonstrated important lessons for organisations that want to build effective cyber-security awareness systems. Similarly, Da Veiga and Martins (2015) described the case study of an international financial institution in which a cyber-security cultural assessment was conducted at four intervals over a period of eight years. The results demonstrated how the security culture of the organisation improved through training and awareness actions. The case study, therefore, illustrated that the cyber-security cultural assessment tool previously developed can be employed in organisations to positively influence the cyber-security culture (Da Veiga & Martins, 2015). Most of the

previous case studies relating to cyber security and the human factor in cyber security emerge from the more security-based literature rather than a behavioural one. This influence is present in the theory and literature used to interpret the results.

3.2.2 Choosing a Case-Study Design

To fulfil the aims of the thesis, this research adopted a qualitative case-study approach. When engaging with an organisation, flexibility in methodology is important. The case-study method made it possible to propose a few different methods, such as interviews and focus groups, to see what worked best for the participants and the organisation. It also allowed for a complete deviation from these methods if it was deemed necessary and it allowed for changes to be made quickly when the COVID-19 pandemic started (see section 3.3 in this chapter for more detail). As discussed further in section 3.4.4, the online environment made focus groups a more challenging method than interviews.

The case study allows for 'how' questions and exploratory 'what' questions. The present research aims to explore and gain insight into the cyber-security behaviours and perceptions. This implies a comprehensive research design with a multidisciplinary character and many variables to be considered rather than controlled and measured. This therefore can be seen as an argument for a qualitative case-study design. The use of a single case study, rather than conducting research with participants from multiple industries and organisations allows the case and context to remain the same while allowing to conduct a deep investigation with multiple questions, methods, use of previous research and theory. The use of different organisations would not have allowed for the same control over extraneous variables, making it harder to separate constructs from context. The context and framework in a single organisation remain the same, allowing for deeper exploration within this environment. Cyber-security perceptions and behaviours are a part of everyday life for those working in large corporate organisations and therefore need to be studied and understood within their own context. Nevertheless, while there are advantages to focussing on one case study, this choice was also influenced by the difficulty in gaining access to organisations generally, and

especially during the COVID-19 pandemic. The context of the pandemic and COVID-19 will be discussed in Section 3.3 of this chapter.

This case study used both inductive and deductive approaches. Despite wanting to investigate the perceptions and behaviours of employees from the ground up, all researchers come into research with orientating ideas (Miles & Huberman, 1994). Coming from a background highlighted in the literature review section, this thesis is naturally shaped by research and theories from cognitive and social psychology and usable security. This was partly explored in section 2.10 of the literature review and the data analysis process is further explored in section 3.6 of this chapter.

3.2.3 The Case Study: The Law Firm

In case-study research the context of the specific organisation has an influencing factor on the participants and findings. The context of the pandemic and COVID-19 will be discussed in Section 3.3 of this chapter. To find a company to participate in this research project, detailed emails were sent out with information for the proposed research to contacts of the supervisor of this project and the PhD student. The contacts were all representatives of private organisations, as government and public sector organisations were deemed to be too broad in scope and culture. The original document of contactable organisations compiled listed 15 companies, as well as some leaders in the cyber-security field. Companies responded with quicker interest than anticipated. The current organisation showed great interest in the proposed research and were keen to move forward quickly. This was seen as desirable by the PhD student and supervisors owing to previous experiences of lengthy processes to get access to organisations. The current organisation further did not mandate the signing of non-disclosure agreements. Hence, it was decided to move forward with conducting research in this organisation, as other leads appeared to have more lengthy processes. It was decided that using one organisation for the research would be methodologically sound, as many of the variables would be the same, or similar (given the changing issues surrounding the pandemic, and remote working). This, along with issues related to the COVID-19 pandemic that will be discussed in section 3.3, led to a single-case

study design, rather than multiple. The decision was made not to name the organisation in this thesis, as to align with other research in the area (for example, Da Veiga & Martins, 2017; Inglesant & Sasse, 2010). However, the organisation did not request this, and the author is aware there may be identifying information throughout the thesis.

The case-study organisation has around 80 offices, with lawyers located in more than 40 countries throughout the Americas, Europe, the Middle East, Africa and the Asia Pacific. Their clients range from multinational, *Global 1000* and *Fortune 500* enterprises to emerging companies developing industry-leading technologies. They include more than half of the *Fortune 250* and nearly half of the *FTSE 350* or their subsidiaries. The organisation also advises governments and public sector bodies. Within the organisation, the cyber-security team sits under the risk department, rather than being a function of IT. See Figure 1 below.

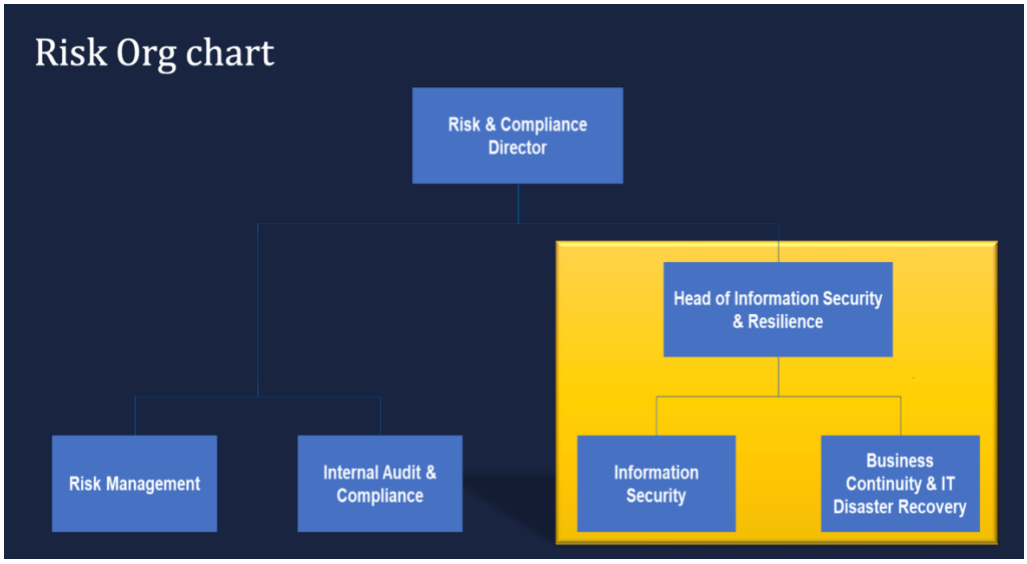

Figure 1. Risk Organisation Diagram

At the time of writing, the organisation was in the process of developing a new cyber-security campaign. However, previous campaigns that participants in this study would have received included initial cyber-security training when they joined the organisation and were sent simulated phishing emails used to train employees to spot phishing emails. The programme

that ran in 2021 included: mandatory awareness training, an optional culture survey, optional proficiency assessment (when employees join the firm) and a variety of workshops.

Many law firms including the current organisation, and other sectors outside law, have a predominant internal divide between the business and fee earning sides of the firm. Fee earners are members of staff who directly generate income for the firm, therefore the fee earners are usually qualified lawyers such as solicitors, barristers or chartered legal executives (Forstenlechner et al., 2009). Fee earners' time is charged against client work. In comparison, the business side of the firm sometimes referred to as the 'support staff' or 'business staff' (for example, departments such as cyber security or human resources) are employees who do not produce revenue for the employer by charging clients. In most major law firms business functions are headed by a strategic level manager with a director title. This person is often a non-practising lawyer with a fee earning background. Below the level of director, are several management levels to manage employees in technical, clerical or specialist roles (Forstenlechner et al., 2009). These distinctions were also present in the case study underpinning this thesis.

Previous research has explored the divide in law firms between fee earners and support staff. Forstenlechner et al. (2009) surveyed the support staff of law firms, finding that "You are either a fee earner or a fee burner" was the key narrative felt by support staff. The authors argued that this mentality often leads to reduced working morale in such staff. This demonstrates that this view of a split between staff resides in law firms (Forstenlechner et al., 2009), though, it is unclear what the implications would be for cyber security if any. Although some of the participants in this study were fee earners, the majority were support staff, or on the business side of the firm. Fee earners were explicitly said to be hard to recruit for interviews and focus groups as this would take time away from the time fee earners were able to bill clients for.

A law firm, as a case study, also has a few other defining features, and some previous research has analysed cyber-security concepts within a law firm. Some researchers suggest that law firms are of particular interest to cyber criminals (McNerney & Papadopoulos, 2012), as law firms house significant stores of sensitive information. Therefore, breaching a single

firm can provide a range of transactional sensitive data for cyber criminals. In recent years, organised criminals have been increasing in their capabilities and now pose significant challenges to large corporations such as banks and law firms (McNerney & Papadopoulos, 2012). Other researchers suggest that trust accounts, public money held on behalf of depositors to be used at the discretion of the trustee, are particularly vulnerable to cyber-security issues (Mubarak & Slay, 2006). However, at the time of writing, research is yet to look at the specific cyber-security culture of a law firm and the legal sector as a whole. In fact, despite the clear interest of law firms to attackers, there have been few in-depth case studies of cyber-security awareness, behaviours, and perceptions in private organisations as a whole.

Another prominent feature of the chosen organisation is that it had previously (within the past four years at the time of research) been the victim of an organisation-wide cyber-attack. The cyber-attack, now known as a global cyber event named Petya or NotPetya, impacted many other organisations, including Russian oil producer Rosneft and Danish shipping company Maersk (Financial Times, 2017; Lika et al., 2018). NotPetya was a remarkably sophisticated 'Supply Chain' attack on a trusted software vendor. The malware was embedded in a standard M.E.Doc software update. M.E.Doc payroll systems are widely used in Ukraine by the government and international companies operating in Ukraine. The current organisation was not specifically targeted, yet over 2,000 organisations were affected worldwide. NotPetya takes on the appearance of the Petya ransomware; it injects malicious codes into computers and then attempts to get administrator access. Once inside a company's system, the NotPetya destruction programme traverses from PC to PC, destroying the infected machines' document systems, with researchers finding that no existing solutions can be used to decrypt the hard disks that had been encrypted by NotPetya ransomware (Lika et al., 2018). For the current organisation, the NotPetya ransomware attack infected computers across its platforms, encrypted all affected files and hard discs, deleted its own encryption keys as it went and requested a ransom in bitcoin to regain access or avoid the threat of deletion (Financial Times, 2017). According to online sources, in 90 minutes, NotPetya caused significant damage. Many servers were hit and required rebuilding. All primary communications systems were affected: email, phones, voicemail, and video conferencing methods. Many applications used by employees were affected, and 6500+ PCs and laptops needed to be wiped and rebuilt or inoculated against infection. Online news

articles stated that the organisation's IT team put in 15,000 hours of paid overtime to recover from the NotPetya malware infection (Crozier, 2018). This changed how the business ran for a couple of months and led to several cyber security-related changes, both technical and behavioural. For example, the organisation is said to have segmented its network so that if they were to get hit again, it would have a greater chance of containing the spread of the attack (Crozier, 2018).

However, little previous research has been done to look at the impact of an actual cyber-attack on employee perceptions and behaviour, especially years after the fact. Previous literature demonstrates how members of the general public perceive and engage with risk and how they are impacted by cyber-attacks (Bada & Nurse, 2020). This research importantly demonstrated that cyber-attacks could have a psychological impact on the general public. One study looked at the emotional reactions of IT and non-IT employees to a 2017 cyber-attack at a global manufacturing company by interviewing employees (Stacey et al., 2021). The research demonstrated that prior to the attack, the non-IT employees did not adhere to the cyber-security policies created by the security team. Post-attack, non-IT employees were said to understand the seriousness of such policies and adhere to them. This demonstrates the possible impact of a cyber-attack on employees (Stacey et al., 2021).

3.3 The Contextual Impact of COVID-19

In March 2020, the UK went into a national lockdown owing to the declaration of COVID-19 as a global pandemic (World Health Organisation, 2021). Between March and April 2020, nurseries, schools, universities, and all nonessential businesses were forced to close, and, during this national lockdown, people's basic rights were restricted by a considerable amount (Zacher & Rudolph, 2021). Since then, this pandemic has altered the lives of many across the globe. This has included an impact on people's wellbeing, the way we work, and impact on research. After restrictions were lifted in the summer of 2020, social distancing remained. The UK then went into a second national lockdown in November 2020, and a Tier system was put in place, restricting meetups and research practice. Further issues also ensued with

further restrictions and lockdowns in December 2020 and January 2021, returning again to a tier system thereafter.

Throughout the entirety of the present research, therefore, restrictions were still in place nationally. It should be noted that the current COVID-19 crisis is a global health crisis, millions of people have been put in far worse situations than delays in scientific research. Social distancing and both lockdowns have been essential in minimising the spread of COVID-19. For many researchers, however, this represented a change in fieldwork methods, either moving away from face-to-face practice or a total stop to research. The first lockdown coincided with the timings of the main fieldwork and primary data gathering for this thesis. Owing to the well documented (Flick et al., 2020; Newington & Metcalfe, 2014) difficulties surrounding finding participants and organisations to openly participate in research, especially without restraining non-disclosure agreements or restrictions on publications, we felt it was too late at this point to change the scope to a different organisation or away from organisational research more generally. However, there were many issues that needed to be considered when discussing the research and the findings and a few research conundrums to be mitigated if the project was to continue.

These issues were largely related to the research methods. The researcher and employees at the organisation were in lockdown and working from home through the data collection period. As interviewees and focus groups could no longer be done in person, they were moved online. The usability and reliability of such methods will be described in section 3.4.4 of this chapter. Additionally, as described in section 2.9 of the literature review, the pandemic has had a great impact on society and the global workforce, such as the change to remote working, wellbeing and the perception and prioritisation of threats. Moreover, the pandemic arguably changed the cyber-security landscape in a number of ways, both in terms of attack methods and vectors, and in terms of organisational abilities to run cyber-security campaigns. The COVID-19 pandemic led to a mass movement to remote working, hybrid working or working from home. Although remote working is by no means a new concept, it has never been seen on the scale it has during this period. This shift in what is considered to be 'normal living', is likely to also impact organisations and employees. Moreover, research reported an increase in psychological and wellbeing issues among the global workforce,

including anxiety and life satisfaction (Reynolds et al., 2008; Sim et al., 2004; Styra et al., 2008). However, it should also be pointed out that for some people, the move to work from home had many positives and the idea of going back to the office is causing increased levels of stress and anxiety. As discussed in the literature review, remote working has also been demonstrated to impact productivity, work-life balance, and wellbeing. This research brings into question the extent to which people's security concerns would change, owing to the increase in other, and arguably more pressing physical and mental health concerns.

3.4 Methods

This section will introduce and discuss the different methods used to explore this case study. This includes the qualitative standards and workings of semi-structured interviews, elite interviews and focus groups. Then the section will look at how these methods were adapted to be completed online and used within the context of a global pandemic. The process and experience of conducting these online interviews and focus groups will be discussed in detail. The organisational and participant recruitment and demographics will also be discussed, as will the ethical considerations and the process for ethical approval.

3.4.1 Interviews

For qualitative researchers, one of the most common methods used for data collection is interviews (Alsaawi, 2014). Interviews are categorised in the surrounding literature in three broad ways: structured, unstructured, and semi-structured. This section will discuss unstructured and semi-structured interviews, as structured interviews yield primarily quantitative or surface-level data. No interview can be seen as entirely unstructured, though some can be seen as merely guided conversation. Unstructured interviews are often used in ethnographic research and are often conducted alongside the collection of observational data (DiCicco-Bloom & Crabtree, 2006). In an ideal unstructured interview, the researcher follows the participant's narration, spontaneously generating questions based on the conversation led by the participant. It is known for the researcher to have a small list of

questions, referred to as an agenda or aide-mémoire (Zhang & Wildemuth, 2009). Unlike the topic guide used in a semi-structured interview, the agenda does not specify the order of the conversation but is just meant to add a small amount of consistency across different interviews (Zhang & Wildemuth, 2009). For example, in the cyber-security literature, Schlienger and Teufel (2003) name unstructured interviewing as a way to analyse cyber-security culture, albeit conducted alongside other research methods. However, the unstructured interview has been criticised for its reliability. Researchers have asserted that the way questions are delivered may impact the answers given, and there may be a lack of consistency between interviews, making data analysis a more complicated process (Alsaawi, 2014).

In comparison to the unstructured interview, where the interview is conducted alongside the collection of observational data, the semi-structured interview is often a standalone method of data collection (DiCicco-Bloom & Crabtree, 2006). The interview is generally set around a detailed topic or interview guide or organised around open-ended questions, with free-flowing questions emerging from the interviewer depending on the direction of the conversation (Barriball & While, 1994). Therefore, this interview technique allows for the use of probes, which further permits the expansion and clarification of topics raised by the participants and allows the interviewer to explore inconsistencies between the participants' accounts (Barriball & While, 1994). This semi-structured in-depth interviewing method is the most commonly used and can be done on an individual level or in groups, as discussed below. The individual semi-structured interview allows the researcher to delve deeply into social, personal, and behavioural matters (DiCicco-Bloom & Crabtree, 2006). The flexibility of semi-structured interviewing makes them particularly suitable for answering why and how questions. Furthermore, probing allows interaction between the researcher and participant, which helps build a sense of rapport. Unlike in the unstructured interview, where rapport is developed over time, the researcher in semi-structured interviews must develop a rapport during the interview. Rapport is needed for the participant to feel safe and comfortable when sharing their experiences, especially if the research regards a topic of sensitivity (DiCicco-Bloom & Crabtree, 2006). The semi-structured interview has been a proven method used in case studies within the cyber-security domain. For example, Khalfan (2004) used a case study

with semi-structured interviews to explore the cyber-security considerations in outsourcing projects in Kuwait's public and private sectors.

This research uses a semi-structured interview method. This interview method, as demonstrated above, allows for topics to be covered and for a degree of flexibility. Flexibility was desirable in this case, mainly because the topic of cyber-security and the perceptions people have on the matter remain largely under-researched and also because it provides a more relaxed atmosphere for the participants.

3.4.2 Elite Interviews

Elite interviews were also used as a method to gather contextual data about the organisation and its cyber-security framework. Elite interviews typically focus on 'elite' members within a business or society. This is because researchers often aim to gain an understanding of the perspectives and behaviours of leaders in business, politics or society (Harvey, 2011) or those with expert knowledge on a specific subject (Van Audenhove & Donders, 2019). Data on how elites perceive cyber security related situations, current standings and how they make key decisions provides a unique perspective that can often not be obtained through other data collection methods (Liu et al., 2020; Parsons et al., 2014). However, there is no clear-cut definition of the term 'elite interview', given its broad applicability. In the current research, the term 'elite interview' is used for two interviews conducted with senior cyber security employees of the organisation. They are elite as they are in senior company positions and highly skilled and knowledgeable in both the context of the organisation but also on the topic of cyber security. This is similar to previous organisational work where the term 'elite' is reserved for those occupying senior management, board level positions and those with expert knowledge (Harvey, 2011; Van Audenhove & Donders, 2019). At the same time, it should be recognised that these views might not represent the views of the whole organisation, and such participants may be prone to a set of biases influenced by knowledge of cyber security and a possible incentive to represent the organisation in a positive light.

A large part of elite interviews involved gaining trust and informal rapport with those being interviewed (Goldstein, 2002). The development of trust and rapport is crucial in interviews, but special consideration is often given to those in elite positions, owing to the time they must give up completing the interview and because of the expert knowledge they must bestow (Goldstein, 2002; Harvey, 2011). The interviewer may need to do more background and topic relevant research with elite interviews, as the interviewee might challenge them on the discussed subject and its relevance. The culture of organisations is often shaped or at least influenced by the elite or dominant coalition (Bowen, 2002).

3.4.3 Focus Groups

Focus groups were also used as a method for data collection in the current research. Focus groups often have similar principles to the semi-structured interview but take place with groups of respondents rather than just one. Focus groups, therefore, provide rich and detailed data regarding the thoughts and perceptions of a group of people in their own words (Freitas et al., 1998). Similar to unstructured interviews, it is argued that focus groups are predominately beneficial when a researcher wants to discover and understand people's views, perceptions and experiences on a particular issue (Dilshad & Latif, 2013; Freitas et al., 1998; Milena et al., 2008). The role of the moderator is to organise, conduct and control the focus group process while allowing the participants to take the focus groups in their own direction if a relevant topic is bought up (Milena et al., 2008). Generally, it is believed that it might be beneficial for the participants to share some common characteristics so that positive interactions may occur and situations where persons dominate may be avoided. If there is an instance of persons dominating the conversation, the moderator's job is to bring other group members into the conversation (Dilshad & Latif, 2013). Rich data can be collected from the focus group methodology with speed, as multiple participants complete the focus group simultaneously. Bauer et al. (2017) used a combination of focus groups and semi-structured interviews to investigate how users perceive cyber-security awareness programs and related implications for compliant cyber-security behaviour.

3.4.4 Online Interviews and Focus Groups

As discussed in Section 3.3, owing to the COVID-19 pandemic and national lockdowns, focus groups and interviews had to be moved online if the research project was to be a 'socially distant method' (Lobe et al., 2020) and be completed within the funding period. To mitigate delays, it was suggested to the organisation that focus groups and interviews take place on Zoom. At the time, this software was the video conferencing tool of choice for the organisation while having good features for conducting focus groups and interviews. This section discusses the implications and supporting evidence for using online video conferencing tools to conduct interviews and focus groups.

Given the ubiquity of the Internet, the qualitative research community has advanced with technology. Researchers use the Internet to conduct literature searches and reviews, telephones to conduct interviews (Novick, 2008), and social networking sites and instant messaging have also created alternatives for interviewing (Stieger & Göritz, 2006). In recent years, video conferencing software for interviews and focus groups has become a new method for data collection (Gray et al., 2020; Ramo et al., 2019). Video conferencing allows participants and researchers to communicate using audio and video in real-time (Gray et al., 2020). There are a number of circumstances where this method is particularly advantageous: when participants are geographically dispersed or live in more rural areas, when funding does not allow for the researchers or participants to travel, in order to interview more participants in a shorter amount of time and to reduce circumstances that could lead to cancellation, for example, weather and travel fees (Gray et al., 2020). Video conferencing, therefore, provides a feasible alternative. During the COVID-19 pandemic, therefore, many qualitative researchers were forced to switch to this method.

Video conferencing generally requires researchers and participants to download or access a specific software online and have access to high-speed Internet. Researchers and participants can then access the chosen software or platform via a device of their choice. There are a number of different video conferencing platforms, including Microsoft Teams, Zoom and Google Hangouts. With the number of platforms available, the researcher must decide which

platforms are best depending on their research needs. For this research, Zoom was chosen for a variety of reasons. First and foremost, the case-study organisation stated it was the software they were currently using. Secondly, unlike Skype, Zoom does not require participants to download the software or have a paid account. Thirdly, Zoom also has a screen share function, which means researchers and participants can share documents like research information forms or aids to show participants during focus groups or interviews (Gray et al., 2020).

Because of the growth in the use of video conferencing as a research technique, especially in the wake of COVID-19, there are now a few research studies evaluating its effectiveness as a research tool. Gray et al. (2020) interviewed participants about their experiences of participating in a parenting programme conducted via Zoom. The participants generally reported positive experiences with Zoom. All participants enjoyed Zoom's video conferencing capabilities and stated that they would be willing to participate in a future Zoom interview. Participants found the fact they could see the interviewer to particularly add to the positive experience. The added benefit of not having to travel to a location to partake in the interview was of particular benefit (Gray et al., 2020). Some researchers have compared face-to-face focus groups with those conducted via online video conferencing. Similarly, Archibald et al. (2019) interviewed participants regarding their experiences with Zoom as an interviewing platform. Several of the participants experienced technical difficulties with Zoom in the interview process. However, most participants described their interview experience as highly acceptable and rated Zoom above alternative interviewing methods such as face-to-face interviews, telephone, and other videoconferencing software. The researchers argue that the findings suggest the viability of Zoom as a method for qualitative data collection because of its ease of use, cost-effectiveness, security options and data management features (Archibald et al., 2019).

Kite and Phongsavan (2017) conducted online and face-to-face focus groups with participants and used reflective practice to assess how and if the groups were similar or different across the two platforms. It was found that the level and quality of discussions were similar between online and face-to-face groups. However, some issues were presented, mainly regarding the technical difficulties experienced by participants and the recording quality to facilitate

transcription and analysis (Kite & Phongsavan, 2017). Lobe and Morgan (2020) conducted a series of online discussions using a video conferencing tool in order to look at the differences between four-person focus groups and two-person dyadic interviews. Results illustrated the value of online focus groups. Four-person focus groups generally produced more unique ideas; however, participants generally favoured the dyadic online interviews. This was mainly due to logistical issues and recruitment issues. Moreover, moderating issues, including nonverbal communications, probing responses, bringing the conversation back to the topic and encouraging non-talkative participants, were also rated more favourably in two-person focus groups (Lobe & Morgan, 2020). Therefore, this is slightly different from in-person focus groups, where historically, researchers have favoured groups of around six (Freitas et al., 1998). However, some of this research was conducted before video conferencing became a massive feature of everyday life. Hence, it is hard to say what role Zoom fatigue might have played in the participant responses of these studies.

3.5 Participants

3.5.1 Selection and Recruitment

In order to recruit participants, the researcher wrote up a recruitment email that the organisation sent round internally to employees with the full information sheets attached (see Appendix 9.2). For the focus groups, the researcher specified getting focus groups from different offices around the firm within the UK to ensure any similarities or differences between office cultures were explored. For the interviews, the researcher specified having interviews with employees across all levels within the organisation. Once volunteers came forward, a list of potential participants and their emails were forwarded from the company to the researchers to arrange whether the participants wanted to take part and the times and dates of the interviews and focus groups if they agreed. The researcher managed all subsequent communication with potential participants.

Importantly, the organisation was not aware of who ended up participating in this research, and any feedback was completely anonymised. The feedback received by the organisation is discussed at the end of this section. Once confirmed, Zoom invites were sent directly to the participants for the date and time agreed, along with the information sheet and consent form to be signed and returned to the researcher before the interview or focus group. Researchers have argued that there is no particular number of participants that need to be interviewed (Alsaawi, 2014). Guidelines for determining sample sizes for interviews are virtually non-existent (Guest et al., 2006).

In total 40 participants took part in this research; all were from the same law firm. 2 elite interviews, 20 interviews (9 management, 11 employee) and 18 participants in the 7 focus groups, from 7 different offices around the UK. See Table 1 and Table 2 for further information on participant demographics, with reference to whether they worked in IT or not, and whether they worked in fee-earning roles or not. Employees came from different departments in the business, and from different offices in the UK.

Participant ID	*IT/F / non*	*FE/B*
FG1P1	Non	FE
FG1P2	Non	B
FG2P3	Non	B
FG2P4	Non	FE
FG3P5	Non	B
FG3P6	Non	B
FG3P7	IT/F	B
FG4P8	Non	FE(p)
FG4P9	Non	FE(p)
FG5P10	IT/F	B
FG5P11	Non	B
FG6P12	Non	FE(p)
FG6P13	Non	FE(p)
FG6P14	IT/F	B
FG7P15	Non	B
FG7P16	Non	B

FG7P17	Non	B
FG7P18	Non	FE(p)

Table 1 . Focus Group Participant Demographics. In participant ID: FG = focus group, P = participant number. In IT/F/non: IT/F = worked in IT or infosec role, non = did not work in IT or infosec role. In FE/B: FE = fee earner, (p) = paralegal, B = business side/non-fee earners.

Participant ID	*IT/F /non*	*FE/B*
G1P1	Non	B
G1P2	IT/F	B
G1P3	IT	B
G1P4	Non	B
G1P5	Non	B
G1P6	Non	B
G1P7	Non	FE
G1P8	Non	B
G1P9	IT/F	B
G2P1	IT/F	B
G2P2	Non	FE
G2P3	IT/F	B
G2P4	IT/F	B
G2P5	Non	FE
G2P6	Non	B
G2P7	Non	FE
G2P8	Non	FE
G2P9	Non	FE
G2P10	IT/F	B
G2P11	Non	B
EI1	IT/F	B
EI2	IT/F	B

Table 2. Interview Participant Demographics. In Participant ID: G1 = lower-level employees, G2 = management, EI = Elite Interviews. In IT/F/non: IT/F = worked in IT or infosec role, non = did not work in IT or infosec role. In FE/B: FE = fee earner, B = business side/non-fee earners.

Organisations were approached at the end of February 2020. The chosen law firm responded at the beginning of March that year. The initial scoping meeting was set to take place at the London office the week commencing the 16th of March 2020. That week the UK went into a national lockdown, putting a complete halt to the research for several months. This delay in research was owing to a number of reasons. The organisation, such as the cyber-security team, had to help with a sudden transition to remote working. This involved a large risk mitigation process that lasted for several months due to the evolving risk landscape during lockdown, both concerning risks posed by working from home and new threats, such as COVID-19 related phishing attacks. This meant that despite any mitigation, the researcher could not start focus groups and interviews until June 2020, and these were conducted online.

Towards the end of the write-up of this thesis (January 2022), the researcher gave a presentation to the organisation regarding the findings of this research. The presentation was a 20 slide PowerPoint and essentially a reduced version of the current thesis. The PowerPoint was presented to two individuals within the information security team of the organisation. The themes were presented, along with a few anonymised quotes. No additional information was presented to the organisation that does not appear in the current thesis. At the end of the presentation, the two attendees discussed with the researcher how the thesis would help the organisation moving forward. It was stated that some of the findings would be taken to the board, and, in addition to giving insights, would help the information security team show how such research added value to cyber-security knowledge within the current organisation.

3.5.2 Interview Process

The elite interviews were the first to take place in March 2020. For the elite interviews, a broad topic guide was constructed (see Appendix 9.1). The interviews took place with those on the cyber-security awareness and training team. These interviews were led mainly by those being interviewed, as the aim was to find more out about the organisation and the cyber-security context. The topics concerned the interviewees' job role, the security culture

of the firm, how the cyber-security department secures resources, cyber-security measures/training and how the data from cyber-security awareness and training measures are used. As noted in section 3.4.2 of this chapter, gaining the trust of the elite interviewees was extremely important. This was done through contact with the interviewees prior to the interview. Furthermore, both interviewees assisted with initial access to the organisation, and so rapport was built during these previous conversations.

The second round of interviews was conducted with lower-level employees and those in managerial positions took place in July 2020. The topic guides were created by formulating the research aim and questions into broad topics, for example questions around threat perceptions, biases, behaviours, and workplace policies were formulated to inform the first research question. However, the topic guides, were meant as *guides* rather than strict questionnaires to be always stuck to by the researcher. Hence, because participants would often mention the company cyber-attack and the impact of COVID-19, questions related to these topics were later added by the researcher. The topic guides for managerial participants compared to lower-level employees were slightly different in wording and the direction of the topics (see Appendix 9.1). For example, top-level managers were asked about the behaviour of lower-level employees and lower-level employees were asked how they thought top-level managers viewed them. Topics covered cyber-security behaviours, policies and culture, attitudes towards employees/managers and resources and cyber-security campaigns. Before the interview began, the researcher went over the interview aims and reminded participants that they could drop out of the interview at any time. There were a few connection problems, especially in the first few interviews conducted. This could be attributed to Zoom being newly introduced to the company at the beginning of the national lockdowns, meaning that participants at the beginning were not yet used to the software. For all types of interviews, some participants had their web cameras off, or when participants' cameras were not off, the camera usually showed a close-up of the participants' faces. Although this decreased the ability to gauge non-verbal cues in some instances, the researcher did not insist on having webcams turned on as this would have opened up more privacy and comfortability concerns given that participants were taking the interviews from inside their own homes. After the interview finished, the participants were sent a debrief form giving the contact information of the researcher and supervisors.

3.5.3 Focus Group Process

Focus groups took place in June 2020. Between 5 and 8 participants were invited to take part in each group, as the invites took account of possible attrition rates. See Table 1 for further details on the final numbers for each focus group. Though these numbers seem small for face-to-face focus groups, the surrounding literature has found that participants benefit from smaller groups when conducted online (Lobe & Morgan, 2020). In addition to this, owing to the busy client-facing nature of a law firm, combined with the additional responsibilities of working from home during a pandemic, the attrition rates for the focus groups were reasonably high. The decision was made to continue the focus groups if at least two participants turned up, as focus groups would be difficult to reschedule. However, if only one participant turned up, that participant was asked to join a later focus group. As was the case during the interviews, some participants had their webcams off during the focus groups. This, paired with Internet speed delays, sometimes made it hard for participants not to talk over each other or for the researcher to know when someone had finished talking. The researcher coped with this by circling back to people who had been interrupted and leaving longer delays between a participant's answer and the next question.

A topic guide was written up for the focus groups, with probes liked to each topic (see Appendix 9.1 for full details). Firstly, the moderator went over the aims of the focus groups and reminded participants that they could drop out of the focus group at any time. The topic guide focussed on personal cyber-security threats, organisational cyber-security threats, behavioural interventions and measures taken to relieve threats. Lastly, the participants were shown three different vignettes these were informational (the passage contained plain information about a phishing attack), narrative (the passage contained a testimonial from some who had experienced a phishing attack) and another narrative message where the passage contained a testimonial from another employee at their firm who had experienced a phishing attack (for more detail on the vignettes see Appendix F in section 9.6). After the focus groups were complete, participants were sent a debrief sheet outlining the aims of the

research as in the information sheet and giving the contact information of the researcher and supervisors should the participants have any questions.

3.5.4 Ethics and Responsible Research

As with all qualitative research, ethical issues had to be considered. The current research had potential ethical implications for the privacy of the participants. It was important to ensure that participants were anonymised and insights given back to the organisation would not be identifiable to any individual. It was also essential to guarantee that participants took part willingly and not under pressure from the researchers or organisation. The researcher raised some initial concerns with the organisation about revealing the firm's identity. However, the organisation informed the researcher that they were happy to be named for research transparency.

This study went through a full ethics review process at Royal Holloway, University of London. This process involves two stages. Firstly, researchers completed and submitted some basic information about the project and six basic 'yes/no' questions to identify any issues of ethical concern. The next stage is the ethical review form, which guides researchers in considering potential ethical issues related to different aspects of the study. Researchers can then either go down a Research Ethics Review panel or self-certification route. The self-certification route is taken if researchers believe there to be minimal risks to participants, the environment/society, or the researchers/institution. Therefore, for the purposes of this study, full ethics approval was sort as the research was being conducted in a large multi-national organisation. The research ethics committee at the university approved the application.

All participants signed a consent form which highlighted that participants would be recorded to benefit transcription and that the results of the focus groups would be anonymised by the researcher and completed a demographics form. Participants were also instructed that they would be able to drop out of the study at any point or refuse to answer a question. All participants signed the consent form and consented to be recorded. All participants

completed a demographics form, which asked about gender, age, nationality, and job title. See the consent form, demographics form and information sheet in appendix 9.3, 9.4 and 9.2 respectively.

Raw interview transcripts were stored on the researcher's personal password protected laptop on VeraCrypt. VeraCrypt is a free encryption software. It can create a virtual encrypted disk within a file or encrypt a partition or the entire storage device and is password protected. Once the interviews were fully transcribed and participants were anonymised, they were moved over to NVivo, a software analysis tool discussed in section 3.7. Raw recordings of the interviews and focus groups were then deleted. The anonymised transcripts are now stored on Figshare with restricted access[2].

3.6 Data Analysis

The data captured was the transcription data of the interviews and focus groups. In total there were 30 transcripts, with around 150,000 words in total. The interviews were semi auto transcribed on a Google Pixel and then later edited by the researcher for accuracy. This process is described in section 3.6.1 of this chapter. Data was analysed using a thematic analysis method conducted on NVivo 12. This process is described in further detail in section 3.7 of this chapter.

3.6.1 Automated Transcription

The transcription of audiotaped interviews and focus groups is a widely used method for making data available in textual form for subsequent coding and analysis is widespread in qualitative research (Halcomb & Davidson, 2006; Poland, 2002). Transcription is vital for the data management process for researchers conducting advanced data analysis or using

[2] https://doi.org/10.6084/m9.figshare.19811047.v1

computer-aided qualitative data analysis software (CAQDAS) such as NVivo (Matheson, 2007).

In general, researchers use manual verbatim transcription as well as researcher notations of participants' actions and nonverbal behaviour (Halcomb & Davidson, 2006). This process was slightly complicated in the current research as interviews and focus groups were conducted over Zoom. As stated previously, in the current research, most participants had their web camera turned off, or when participants' cameras were not off, the camera generally just showed a close up of the participants' faces, so the notation of non-verbal cues was not attempted. Furthermore, many researchers experience issues with manual transcription, mainly the time it takes to write out transcripts verbatim. Transcription is considered to be an extremely time-consuming chore (Tilley, 2003). This is often especially the case when researchers have previously engaged with the content of the interview during the interview itself.

Researchers have recently explored the use of automated methods to reduce the task of transcription (Bokhove & Downey, 2018; Da Silva, 2021; Moore, 2015). Such researchers compared transcripts produced by the software and manual transcripts to gauge accuracy. It was found that there were often slight mismatches between manual and auto transcripts. However, it was also found that such mismatches were easily identifiable and easily rectified when researchers reviewed the automated transcripts and rectified any mistakes (Bokhove & Downey, 2018). It was found that the automated transcript process provided great time and cost advantages, even with the needed editing of the first production of automated transcripts (Bokhove & Downey, 2018). Research finds that the process produces 'good enough' transcription for a first version, which can later be edited (Da Silva, 2021).

However, there is an issue with the use of cloud-computing services, as such services produce issues concerning the privacy and confidentiality of the data. This is certainly the case in the present research, where third party access to participant data would be particularly concerning for the organisation. Furthermore, the project concerns cyber security, so the cyber-security practices of the research should be sound. Maintaining the confidentiality of participant data is an established principle in research, and the assurances

given to participants concerning anonymisation and confidentiality must be upheld. Da Silva (2021) researched an automated transcript option that provided a secure alternative while reducing by more than half the transcription time for the researcher. This research, therefore, followed in the footsteps of this method, which is described below.

3.6.2 The Transcription Process

This transcription process follows the method used by Da Silva (2021). Firstly, a Google Pixel 3a device was borrowed from the Information Security Department of Royal Holloway, University of London – the researcher's host organisation. The device was brand new and therefore did not have any pre-existing accounts or data attached to it. The researcher signed into the phone with a new Google account set up for this purpose and downloaded the free applications from the Google Play app store: Google Recorder software, Microsoft Word and Microsoft Outlook. When the interviews took place via Zoom, the Pixel was placed on aeroplane mode to reduce any risk of automated synchronisation of the audio and transcription data. However, Google state that data from the recorder application is only ever stored on the device and is not synchronised (Da Silva, 2021). The recorder was then turned on, and automated transcripts were produced in real-time as the interview took place. Once the interview had been completed, the transcript text was copied and pasted into a Word document on the device and saved onto the device itself. The document was then attached to an email using the Microsoft Outlook app on the device (configured to use the researcher's Royal Holloway University account; no other email accounts were configured on the device) and sent to the university email address (Da Silva, 2021). The researcher was careful to make sure it was only sent to themselves and not any other recipients. The device was then taken off aeroplane mode and connected to the researcher's secure home Wifi network in order for the email to be able to send. The email was then opened on the researcher's laptop, and the text transcript file was downloaded (Da Silva, 2021). The email was then deleted from the inbox and outbox and the deleted items folder. A copy of the word document was then made. The copy of the document was then opened, and the audio recording was played back off the Pixel. As the audio recording played, the transcript was edited, corrected, and anonymised. The transcript was also sectioned, so it

was clear when the interviewer was talking and when the participants were talking. Until all the transcripts were edited and anonymised the automated transcripts were stored on VeraCrypt, as discussed in section 3.6.1. Once all transcripts were edited and anonymised, they were uploaded onto NVivo 12.

The transcription required a high degree of concentration but took significantly less time, as found by Da Silva (2021). It took around 1 hour to edit a 30-minute transcript, something which usually would have taken around 4 hours. The use of this method for this research supports Da Silva (2021), finding there to be a significant benefit to using this transcription process. Not only did the method save time for the researcher, but automated transcription took place while addressing security concerns of cloud-based services. However, there were a few limitations of the method. Firstly, the software is restricted to the English language. It was further noticeable to the researcher that the software also transcribes certain British accents more accurately compared to others. For example, Scottish accents are transcribed less well. This finding is something also established by Da Silva (2021). This was similarly the case for non-native English speakers. In these cases, the process of editing and correcting the transcript took a lot longer.

3.7 NVivo and Thematic Analysis

With large data sets, manually conducting qualitative analysis is not always practical. Over the last few decades, the ability of computer software to assist researchers in conducting qualitative data analysis has greatly improved (Leech & Onwuegbuzie, 2011). These programmes are broadly referred to as computer-assisted qualitative data analysis software (CAQDAS). NVivo, used as a tool for the analysis of the current data, is one such computer programme that assists in storing, indexing, sorting, coding qualitative data and comparing categories and codes based on defined features of participants or transcripts (Leech & Onwuegbuzie, 2011). NVivo does not analyse the qualitative data for the researcher but assists in the analysis. The researcher took a two-day training course in NVivo at the University of Surrey in order to learn how the software works to a higher level.

A thematic analysis was conducted as set out in Braun and Clarke (2006) in their widely cited paper. In the current study, this was done via the use of NVivo 12. Thematic analysis identifies and analyses patterns across a qualitative data set rather than within a particular data item, such as an individual interview or one focus group (Braun & Clarke, 2006). By doing so, thematic analysis organises and describes data in rich detail, helping to interpret various topics within the research. In thematic analysis, a theme captures something significant in the data in relation to the research aims and represents a patterned response.

The current study uses thematic analysis to report experiences, perceptions, and the reality of the participants, rather than attributing examining how these meanings are the effects of discourses within society group (Braun & Clarke, 2006). The current study used both inductive and theoretical thematic analysis (Braun & Clarke, 2006) as perceptions and behaviours were both understood from a ground-up approach, while at the same time, interpretations of the data were made based on previous literature and established theory. For example, the findings around biases were not constrained by the literature presented on biases in the literature review section. Rather, the biases already tested on the field were also the biases that emerged in the current research.

The researcher wrote an analysis research diary to keep track of the analysis process in order for the process to be open and easily replicable for readers. This was done on NVivo in the Notes, memos section of the software. Firstly, the researcher added all the final data files (transcripts) in different folders, one folder for elite interviews, one folder for focus groups, one folder for managers from the interviews and another folder for lower-level employees from the interviews. The researcher then familiarised themselves with the transcripts by reading through them. With regards to the interviews and focus groups, the researcher then began autocoding each file to create cases for the participants and interviewer - beginning with the focus groups and then the interviews. The researcher then went on to add attributes to the cases, adding attributes that would add layers to the research. The attributes regarded whether the participants were in IT roles and their job level (whether they were managers or lower-level employees).

The researcher then began the thematic analysis coding process, following broadly the steps set out in Braun and Clarke (2006). Firstly, the researcher went through two transcripts as a pilot to see how the coding method would work. Secondly, two folders in the codes section of NVivo, titled 'study 1 early codes' and 'study 2 early codes' and used these folders for the first round of coding. As the researcher made codes from the data, different types of coding were used, mainly descriptive coding but also In Vivo coding. In vivo coding places emphasis on the actual spoken words of the participants and can help to highlight how certain words and phrases are used in certain contexts (Manning, 2017). Descriptive coding is also a first cycle method of coding whereby codes represent the topic of conversation being spoken about in the data (Holton, 2007). Codes were grouped as the first round of coding progressed if they related. However, the first round of coding produced many top-level nodes, and a second round was needed to go back over and group these. This is where the degree of coding saturation was observed; where the researcher started to see the same information or themes they have already obtained from previous interviews (Alsaawi, 2014).

Thematic and coding saturation is achieved when the analysis of results reveals no new themes. There may be small new pieces of information or small lower-level codes, but these are not large or relevant enough to constitute their own theme. The themes themselves need to be sufficient to support the conclusions of the research and therefore need to be backed by data. The researcher was able to see the numerical degree of saturation for each code and overriding theme in NVivo as the software tells you how many files (in this case, this would refer to the number of interviews or focus groups) and how many references (how many quotes have been attributed to the specific theme) were appearing in each code and theme. In general, for the higher-level themes, themes were present in at least five files. However, it should be noted that although this was the general trend, themes were not decided on purely because of the number of files or references, which could be arbitrary presented on their own (Lowe et al., 2018) but because of the richness and significance of the data within these themes. Braun and Clarke (2021), whose thematic analysis method (Braun & Clarke, 2006) the current research used, disagree with attempts to 'capture' data saturation purely numerically. Braun and Clarke (2021) argue that their approach to thematic analysis is based on assumptions around meaning. They argue that meaning requires interpretation, in that meaning resides at the intersection of the data caught and the

researcher's contextual and theoretical knowledge. Therefore, attempting to predict or state the point when data is saturated cannot only be based on or tied to the number of references or files or interviews and focus groups. The meaningfulness of any theme derives not only from the dataset but also from the researcher's interpretation (Braun & Clarke, 2021). Moreover, themes do not exist in total isolation from each other but are all part of a broader narrative that aims to present evidence or insights into the research questions at hand. Thematic analysis is also a reflexive organic process, where the analysis could never be considered 'complete', as it never reaches a fixed endpoint. The researcher has to make a decision, based on their own judgment, when to stop coding and move on to creating themes, when to stop creating themes and begin mapping the thematic relations to each other, and when to start writing up the final results.

The researcher started with the coding of the interview employee group. Once the transcripts were finished, the researcher coded the management interview group to the same Nodes - adding some additional codes as the process developed. This is because, although these are different data sets, many of the same topics were spoken about. Furthermore, the research was less focussed on the specific difference in topics but more on the difference in how these topics were spoken about and framed; for example, positive and negative attitudes or how many people viewed a certain topic in a certain light. The same process then took place for the focus groups; however, these codes were conducted separately in a new coding folder, given the aims of the methods were slightly different. In the second round of coding, lower-level codes and higher-level codes were grouped to create more succinct themes, with subthemes created underneath. At this point, similarities were noticed between the themes in the focus groups and interviews. Lastly, the researcher conducted meta-coding over both the interviews and focus groups as both methods had produced similar themes. This process included amalgamating the themes from each method to produce the flow of themes presented in the findings chapter. The interviews and focus group themes were put into the same folder in NVivo, with an overall Node for interviews and focus groups for each theme, so the researcher could still see what data came from each part of the research. See Figure 2 below for an example of how the Nodes were displayed on NVivo 12 for one of the main themes (the individual human element). A screenshot of all high-level codes in the current as displayed in NVivo 12 can be found in section 9.7 (it should

be noted that the exact names of the themes were changed multiple times during and after the writing of this thesis and so may not be the same in the appendix).

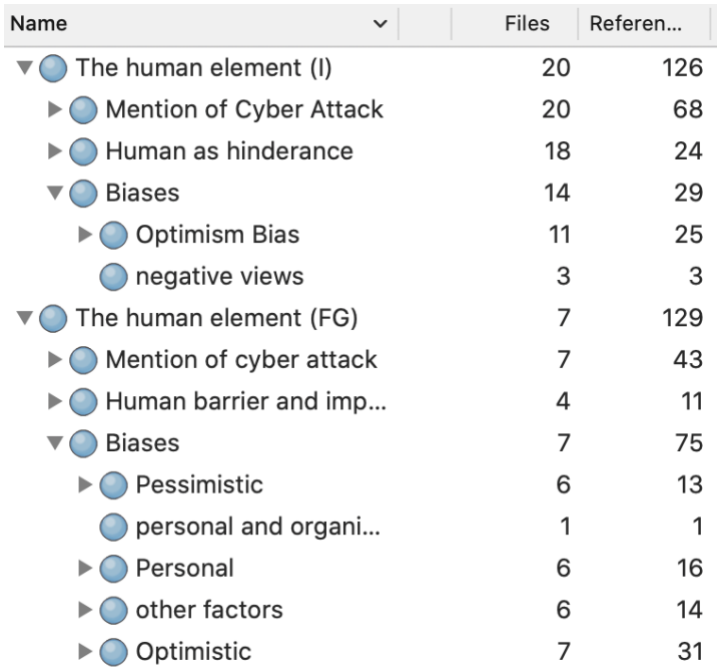

Figure 2. Example of Coding on NVivo 12. Individual Human Element Nodes. The human element (I) refers to the interview data Node and the human element (FG) refers to the focus group data Node.

Four distinct themes arose from the analysis. These themes were a) organisational perceptions of security culture, b) the individual human element, c) perceptions of cyber-security training and policies, and the COVID-19 pandemic and the move to remote working. The first theme includes findings surrounding the social aspects and dynamics of cyber security within the organisation; in this case, this relates to the social norms, social descriptions, and shared experiences (McAlaney et al., 2016) of how cyber security functions within this organisation. The second theme relates to the more individual human element; cognitive thinking patterns and individual views of different aspects of cyber security. The third theme brings together data where participants gave their views on the relevance of cyber security to their job role and cyber security organisational policies and training. Finally, the last theme looks at how participants believed they had been impacted by the COVID-19 pandemic and the impact of the pandemic on cyber security. These themes will be described

and discussed in the following four chapters. Although these themes, along with their relative subthemes, are described separately in the next chapters and are positioned as standalone themes, they are also meant to describe the cyber-security perceptions and behaviour of participants in an interconnected way. As with all thematic research, some of the subthemes had more data to support them than others, when this is the case in the current research this will be highlighted. For example, when there is a small number of participants supporting a view (five or less) the research will highlight that only a minority of participants supported the view. When there is a higher majority than is usual (over 20 participants) this will also be highlighted.

With regards to the elite interviews, these were coded post the primary coding of the non-elite interviews and focus groups. The elite interviews mainly aimed to give context to the study as a whole. It was not until the researcher saw that some of this data could embellish findings of the wider themes that they were included in this way. However, the data and quotes within the elite interviews did fit well with the themes that emerged from the main interviews and focus groups and were combined and are hence presented together within these results. Many pieces of data from the elite interviews fit into themes within the wider coding. However, not all themes were able to be embellished by the elite interviews. This could be for a number of reasons. Firstly, there were only two elite interviews, meaning that there was less data here compared to the focus group and interview data. Secondly, elite interviewees may not have had the same experiences as general employees who do not have expert knowledge of cyber-security behaviour, awareness, and training. For example, as it will be demonstrated, it was interesting to see that employees viewed phishing campaigns positively and compare this to descriptions of the campaigns in the elite interviews, where it was stated that they have attempted only to report phishing campaigns positively.

3.8 Methodological Limitations

3.8.1 The Limitations of a Case Study

This research used a qualitative case-study method. It has been argued that the case-study approach to research is most usefully defined as the intensive study of a single unit, or a small number of units, i.e., the case/s, for the purpose of understanding a larger sector of similar units, i.e., a population of cases (Gerring, 2006). While this method has many merits and proven applications, as demonstrated in the previous sections, the method is notwithstanding limitations, mainly relating to concerns around the validity and reliability of the method.

The fundamental issue of objectivity of the researcher is often highlighted within the surrounding research; in case-study research, the researcher is in danger of losing objectivity by becoming too involved with the case/organisation. This then creates a bias in the results, where the researcher may become an advocate for the case rather than an observer, leading to results that are essentially a product of the researcher's prior experience and prejudice (Meyer, 2001). However, other researchers have argued that this specific issue can be mitigated by recognising and pointing out such presuppositions and making reference to how they may have impacted interpretation (Meyer, 2001). The research and presuppositions that influenced this research are demonstrated in the literature review section of the research, as this previous knowledge will have influenced the researcher's interpretation of the results. This was, however, partially intentional as the researcher also wanted to see how far specific cases fit into previous quantitative and qualitative research as well as previous theories regarding cyber-security perceptions and behaviours. Furthermore, other researchers argue that case-study research, which seeks to describe and make sense of the world, does not require absolute objectivity, as building rapport with the interviewees and sensitivity to and knowledge of the subject at hand is an integral part of the research process (Meyer, 2001). Hence, complete objectivity would reduce the usefulness of the case study.

The lack of generalisability to wider populations is probably one of the most prominent criticisms of case-study research. It has been argued that research is only worthwhile to the extent that it is comprehensive and general, as the research aims to use data to explain phenomena outside the specific context and scope of one study (Miles, 2015). Therefore, a case study is often considered too contextualised and specific to draw scientific conclusions from. However, this potential weakness has been disputed by researchers (Yin, 2009). It has

been argued that it is the purpose and meaning of the data in a case study that determines its value (Miles, 2015). If its purpose is to develop propositional knowledge, then case studies are perhaps methodologically limited. However, if it is to develop understanding and extend knowledge of experience, then the same disadvantage does not exist (Miles, 2015). Furthermore, while quantitative statistical findings are often generalised to other populations, case studies tend to be generalised to other situations with the help of deep analytic investigation. Case studies are not intended to be broadly generalised in the way that surveys or experiments are, which draws into question whether this is a research value that a case study should be measured against (Wikfeldt, 2016). Claims made from case studies cannot, and are not, considered to be proof in a scientific, statistical sense, but they build premises which may be used to make assertions about situations parallel to the one studied (Yin, 2009).

Such biases and issues regarding generalisability and objectivity are perhaps more likely with the use of a single-case study (Eisenhardt, 1989) as used in this research. Another way to 'protect' against such biases would be to use more than one case. However, the desire for depth implies that the number of cases examined in a piece of research must be few (Meyer, 2001). Furthermore, as discussed, gaining access to research more cases would have been difficult owing to COVID-19 and related lockdowns. A positive side-effect of studying a single case is that it allowed for a deeper investigation and analysis of the original case, which in hindsight, turned out to be a beneficial circumstance.

3.8.2 The Limitations of Focus Groups

In addition to the general concerns regarding case studies, researchers also demonstrate that the specific qualitative methods used within this case study: focus groups, interviews, and elite interviews, also have limitations. This section will look at the possible limitations of the focus group method used in the current case-study research.

One of the main problems with the use of focus groups is the possibility that participants will simply reproduce normative discourses or those they believe to be socially desirable, thereby

leading to the group dynamics of the group obscuring more controversial perspectives (Liamputtong, 2011; Smithson, 2000). This can often be the case if there is one 'dominant' voice in the group, meaning that their opinion is the only one that is articulated and is not necessarily representative of the other members' opinions (Liamputtong, 2011). This does not always originate from one individual but may arise because of group members wanting to conform with one individual and therefore replicating one person's opinion (Lezaun, 2007; Smithson, 2000). When this occurs, the moderator can encourage other group members to talk, for example, asking someone who has not spoken directly for their opinion (Liamputtong, 2011). However, it is also important not to make group members uncomfortable, and participants should not be forced to answer a question if they do not want to. The moderator may also want to highlight that there may be diverse opinions on the topic they are speaking about, therefore allowing others to give their opinion comfortably (Liamputtong, 2011). In this research, the researcher followed this protocol and would ask others for their opinions to get them more involved in the group discussion.

Similarly, focus groups are often criticised for offering a shallower understanding of a particular issue than, say, one-to-one interviews might (Lezaun, 2007). Personal experiences may not be discussed, either because of the dominant voice problem or simply because there is not enough time for everyone in the group to delve deep into their own experiences (Liamputtong, 2011; Smithson, 2000). However, focus groups do allow for a greater number of people to discuss their experiences and so finds a balance. Furthermore, this is one of the reasons why the individual interview method was used in addition to focus groups; to ensure detailed accounts of individual experiences were analysed and a larger number. On a more practical level, focus groups can be difficult to organise. Therefore, this can take away from the perceived ease of timing of focus groups compared to interviews, as one has to consider the time it might take to organise such groups. Despite these limitations, valuable data can be gained from focus groups, especially if the moderator is able to manage the group interaction. Although the risk of a dominant viewpoint prevails, participants are encouraged to interact and converse with each other and not merely respond to the researcher. In this way, a larger range and complexity of attitudes and beliefs may emerge (Dilshad & Latif, 2013).

Moreover, the use of focus groups does raise some ethical dilemmas stemming from the degree of disclosure that is possible. In qualitative research generally, the fact that design and methods are largely emergent, rather than pre-specified, as is generally the case with quantitative research, makes it hard to provide fine-grained detail on what will occur in a study (Sim & Waterfield, 2019; Wiles, 2012). This applies even more when we consider focus group research because what is discussed in the group depends in part upon participants, who may unexpectedly raise issues not necessarily intended by the moderator. Of course, even though focus group participants are able to decline to respond to a particular question or comment on a particular topic, arguably more easily than in an interview, they may not be able to divert the discussion away from a topic that they find uncomfortable (Sim & Waterfield, 2019). Moreover, when information is disclosed, there is no guarantee that individuals in the group might speak about what they heard outside the focus group setting. In order to mitigate against this, researchers need to ensure participants know the focus group will contain other people, and they may ask participants to not repeat what was discussed (Sim & Waterfield, 2019).

There is also debate in the focus group literature on whether focus groups give more valid data if the members of the focus groups are friends or strangers (Jones et al., 2018). Focus groups made up of friends may offer a more honest and open discussion among participants than do focus groups made up of strangers, simply because the comfort level among the participants is higher (Jones et al., 2018). On the other hand, focus groups made up of friends may enable participants to identify each other afterwards (Sim & Waterfield, 2019), a situation which is more easily dealt with via the use of pseudonyms in focus groups made up of strangers. However, there is little, if any, data directly comparing the quality of data obtained between the two. Of course, the current research is organisational, and so it is likely the participants were neither friends nor strangers but colleagues, meaning that attempting to make up a focus group of friends or strangers would be difficult.

3.8.3 The Limitations of Semi-Structured Interviews

The interview is a well-known qualitative method that is not exempt from criticism. For example, it is well acknowledged that interviews are time-consuming. The researcher needs to go through an extensive process, starting from establishing access, in this case with both the organisation and the participant, to making contact with participants, conducting the interviews, again, in this case online, which dragged the process out further, followed by transcribing the data (Alsaawi, 2014). In comparison to a focus group, where this process will end with insight from multiple participants, one interview is data from one person. However, as discussed, interviews provide a more in-depth oversight.

In addition, interviews are a co-constructed method, where the interviewer and interviewee contribute to the interviews meaning (Alsaawi, 2014). The interviewer, therefore, must be careful in both how they ask the questions and how they interpret the responses of the interviewee. The interviewer can easily insert bias and therefore need to ensure they protect against this in the way questions are worded and the data analysis. Again, the researcher must counter-act this potential bias by making their assumptions and interests in the subject at hand known.

Others have criticised the semi-structured interview for redefining topics and questions as the interviews and research process progresses. This criticism applies to the interviews captured in the current research, as questions and topics were added during the data-gathering process, in part due to the changing circumstances of the organisation due to COVID-19. From a quantitative perspective,, this criticism stands; changing questions halfway through a survey or hypotheses in a large-scale experiment could render all the previously gathered data useless (Diefenbach, 2009). However, qualitative research is, by nature, explorative. Interesting topics might only come to light after a while of investigation, and the right questions to ask or the right way to word them might only become apparent later (Diefenbach, 2009). Therefore, it can also be argued that qualitative researchers should be encouraged to reformulate research questions and challenge their own assumptions throughout the research process.

There also could be some limitations when comparing focus groups and interview methods. Given what has been discussed in these limitation sections, it may be plausible to argue that

participants may be inclined to reveal different information depending on whether they were in a focus group or an interview. In this way, interviews might result in a less normative discussion (Liamputtong, 2011; Smithson, 2000). However, the case can be made for using both, as the discussion of topics in focus groups may help remind individuals of experiences and points that they also want to bring to the table. This assisted discussion might prove helpful with a complicated topic such as cyber security. Based on this idea, therefore, the theoretical possibility that you might get different information in the interviews and focus groups could make a case for using both methods. Moreover, the researchers did not note significant differences between the dialogue in interviews and focus groups.

3.9 Reflections

Broadly, this research aimed to gain a deeper understanding of cyber-security behaviours in an organisation through the lens of cognitive and social psychological theory and usable security. Originally, the research proposed a mixed methods approach, aiming to use complimentary quantitative and qualitative methods to investigate the research topics and two studies were conducted by the researcher before the start of the research presented in this thesis. These two studies were the beginning of the research journey and were very much pilots for the research presented in this thesis. However, we decided to not include them in the main thesis owing to several weaknesses in the studies' methodology and scope. However, given that these early arrangements shaped the scope and direction of the research, this section briefly reflects on them.

The first focus group study conducted utilised a thematic analysis of in-depth data from four focus groups with 14 adults in the UK. The research revealed a variety of PMT constructs and cognitive biases in relation to cyber security. It showed that people are optimistically biased and fatalistic in their thinking of cyber-security threats. It also revealed that the communication and messaging of such threats often fail to account for such biases. However, the scope for this study was too broad, participants came from a variety of organisations and backgrounds, creating no distinct context on which to abstract the results. Secondly, the sample was convenience based, which can lead to bias, and reduce the generalisability of the

findings. The convenience sample also meant that, although not intentionally, participants were with others of a similar age within focus groups. Thirdly, because of the lack of context, it was found that after analysis the results did not contribute anything of great significance to the research field. These were all lessons learned from and contributed to the development of this thesis.

From the previously undertaken research and the surrounding literature, a significant gap in the literature was identified. That is firstly, there being a lack of deep qualitative research looking at perceptions, biases, and behaviour in cyber security, particularly in the context of organisations. This was even more notable when considering the stance of many pieces of previous research, in that much research seems to take a 'human as a problem' standpoint, rather than a 'human as a solution standpoint' (Zimmermann & Renaud, 2019). We therefore decided to approach organisations in order to conduct research as a case-study approach in order for the exploration of cyber-security perceptions and behaviours within real-life settings.

The second study completed within the context of the PhD was a survey. Based on this previous research finding the existence of the optimism bias in reference to cyber security-based risks, this study set out to test two different strategies for reducing the optimism bias in the information-security domain. One survey was created to be used in this experimental study was generated based on previous relevant optimism bias literature. However, the survey's reliability and validity were not tested through factor analysis or other means, furthermore the findings demonstrated only that the optimism bias appeared in relation to cyber-security risks. Moreover, we noticed a gap in the literature in that most research looking at the optimism bias was quantitative and not done within the context of an organisation or research amongst other factors. Hence, because of the direction the PhD was taking, i.e., that of a qualitative nature, the researcher also chose this study not to appear in the final thesis, although it did assist in shaping the final literature review and its aims.

Based on the lessons learned from the two previous studies conducted early in the PhD, the research took a new turn. The researcher therefore decided to approach organisations in order to conduct qualitative research on cyber security relating to usable security and

psychology within an organisational context. Our original research proposal to the organisation consisted of three studies, relating to a few elite interviews and two separate studies. However, all studies were inter-linked, and it was assumed that data from all three studies would be useful towards the three different sets of aims. Later, we decided to conceptualise the research as one case-study with different methods, which is how it is presented in the current research write-up. To gain an overview of the cyber-security awareness context, we firstly aimed to conduct a few elite interviews with those in cyber-security awareness roles. The first main study then aimed to gain: a deeper understanding of the optimism bias in an organisational context; an understanding of whether this bias still exists in a company that has been a) focused on cyber-security behaviour change and b) victim of a large ransomware attack; and lastly gain an understanding of the opinion of techniques that could be used to change or foster the optimism bias. The second study aimed to: understand how the human-centric approach manifests in managers and employees; understand psychology of management, and what management think the psychology of employees is like – see where/if optimism biases fall, see if they see employees as solution or problem; understand the thoughts and behaviours of lower-level employees regarding their behaviour and company cyber-security policy and to see if managers understanding of employees' matched employee behaviours. However, as the research progressed this came to be seen as one study, with similar aims, but utilising different methods throughout; elite interviews, interviews and focus groups.

3.10 Upcoming Research Themes

In the next section, the four distinct themes that arose from the analysis will be described and discussed in terms of their relation to the psychological theory and cyber-security literature discussed in the introduced of this thesis. The themes are named as follows: a) organisational perceptions of security culture, b) the individual human element, c) perceptions of cyber-security training and policies, and the COVID-19 pandemic and the move to remote working. The first theme includes findings surrounding the social aspects and dynamics of cyber security within the organisation; in this case, this relates to the social norms, social descriptions, and shared experiences (McAlaney et al., 2016) of how cyber

security functions within this organisation. The second theme relates to the more individual human element; cognitive thinking patterns and individual views of different aspects of cyber security. The third theme brings together data where participants gave their views on the relevance of cyber security to their job role and cyber security organisational policies and training. Finally, the last theme looks at how participants believed they had been impacted by the COVID-19 pandemic and the impact of the pandemic on cyber security. These themes will be described and discussed in the following four chapters. Although these themes, along with their relative subthemes, are described separately in the next chapters and are positioned as standalone themes, they are also meant to describe the cyber-security perceptions and behaviour of participants in an interconnected way.

3.11 Summary

Overall, this chapter summarised the methods used in the current research for both data collection and analysis and some possible limitations with the chosen methods. This section also discussed the implications of doing research within and during the pandemic and the research journey of which the current research is the result. The current research presents research from a case study. The analysis of the focus groups and interviews produced four main themes: Organisational perceptions of security culture, the individual human element, perceptions of cyber-security training and policies, and the COVID-19 pandemic and the move to remote working. These themes address the research aims and questions of the current research as they describe cyber-security culture, perceptions, biases, and behaviours of this organisation. The following four chapters delve into these four key themes and their subthemes and discuss their relevance to theory and research, as well as how they have substantiated previous work.

Chapter 4. Organisational Perceptions of Security Culture

4.1 Introduction

This chapter looks at the subthemes and findings grouped within the theme of organisational perceptions of security culture. Organisation aspects, in this case, relate to the social norms, social descriptions, and shared experiences (McAlaney et al., 2016) of how cyber-security functions within this organisation. For example, beliefs surrounding the culture of an organisation and how the cyber-security team functions are explored. As discussed in the literature review, security culture is defined in many ways throughout the literature and lacks a shared understanding. However, these definitions generally all include a reference to the social context surrounding cyber security in which individuals operate (Ruhwanya & Ophoff, 2021). For the purpose of this case study, the researcher differentiates between the organisational aspects of cyber security, on the one hand, which will be discussed in this chapter and the more internal and cognitive perceptions and individual aspects on the other, which will be discussed subsequently in Chapter 5. Although both these chapters relate to psychological processes, the social/cultural aspects deal with employee views and the functioning of their environment. In contrast, individual cognitive psychologies focus more on internal mental processes and understandings (DiMaggio, 2013). The social layer (Gioe et al., 2019) within security culture refers to how employees or specific departments view each other or interact and the social differences between groups.

The themes discussed below are social organisational aspects related to cyber security; how participants view their external cyber-security environment. The first theme discussed is '*good and strong': direct references to security culture'* (section 4.2). This first theme demonstrates how participants generally saw the culture of the organisation to function positively and safely. The second theme, entitled *'responsibility: 'It's managed for us'* (section 4.3) looks at the general understanding that the cyber-security team manage cyber security behind the scenes. The third theme *'separate but accessible; how Infosec functions'* (section 4.4) demonstrates that participants feel cyber security is separate from them, but that they are able to access the team if needed. The last two themes *'lawyers are different:*

cultural differences in cyber security' and *'law firms are different: cultural differences in cyber security'* (sections 4.5 and 4.6) look at perceived cultural differences between job roles within the organisation and perceived differences between law firms and other sectors. Altogether, these subthemes make up the wider social culture theme as seen in the data.

Within the subsequent findings chapters, anonymised quotes from the data are used to demonstrate themes and their subthemes. The quotes are illustrative and will provide specific examples of the themes and subthemes. The researcher attempted, where possible, to choose succinct quotes that were representative of both the of sentiments participants and patterns within the data. The used quotes have not been edited and are, therefore, in general, verbatim. However, small grammatical errors and repeated, or random, words that do not add to the quote have been edited to make the quotes understandable for the reader, as is routine in qualitative research (Lingard & Watling, 2021). When the quotes refer to a concept not stated within the quote, the concept will be highlighted within square brackets. Moreover, ellipses are used in the middle of a quotation to indicate that part of the quote has been omitted original sentence. This has only been done where a quotation includes a digression not germane to the point being made, and care was taken to ensure the preservation of the original meaning of the quotation. Where the existence of a subtheme is not made up by many participants (more than 5), this is highlighted. However, these findings are still important as they reflect differences and non-consensus within this case study.

4.2 'Good and strong': Direct References to Security Culture

Although most themes within this section have relevance to the security culture of the firm, for example, perceptions of the human element and training might pertain to general cyber-security culture, the current theme pertains specifically to participants referencing and describing the 'security culture' of the firm directly. Many participants pointed directly to the idea that the firm's culture was 'strong' or 'good'. However, when trying to elaborate or if pressed further, participants did not generally come up with specific reasons why they believed this was the case, G1P7: *'I think it's actually for a law firm really good and I mean again, I don't have you know figures or anecdotal evidence to support that'.* When

participants did give examples, these were often related to physical security. One participant started by saying the culture was good/strong but then gave an instance where their behaviours might be considered not to be up to standard.

> G1P6: *'Um I think it's pretty strong and I mean in addition to like company data, there's also physical security that they take quite seriously and so we're not supposed to really let anybody tailgate into our office they need to buzz in I mean, technically that rules for absolutely every person but obviously if it's the guy sit next to, and he's arrived at the same time. I don't make him buzz in with me. I just let him in…'*

On the other hand, some participants put the reasons they thought they had a 'good' security culture within the firm down to a general feeling they had without specific evidence to back this up. Others put the belief that the security culture of the firm was good down to the fact they felt they had good cyber-security programmes and the fact they felt people were generally well educated within the firm, demonstrating a belief that collective knowledge throughout the firm on cyber security was good. However, others suggested that the policies and programmes were not the organisation's strong points, demonstrating mixed considerations for why the security culture is considered good.

The elite interviews also included data on security culture. When EI2 spoke about the security culture, they perceived their organisation to be ahead of other firms. EI2 believed their organisation to have a good level of phishing reporting. Moreover, it was stated that the new cyber-security awareness programme they were running focussed on the human factors of security. On a higher level, EI1 suggested that leaders within the firm wanted the information security department to grow and that they themselves and others within the risk department had not been given the hiring freeze that all other departments had been given owing to COVID-19. They argued that this signified a focus on cyber security from leaders within the organisation. However, EI1 and EI2 also said that overall they believed the culture to be poor, or at least low on employees' agenda in general. EI1 viewed that employees had an 'out of sight, out of mind' thought process regarding cyber security.

EI2: *'The security culture is… we're very much ahead compared to a lot of firms but like everybody, it needs a lot of grading yeah, for the culture… the culture is it's quite poor…'*

EI1: ''*Um low on people's agenda* [cyber-security culture]*. That would be fair to say at the moment. We get really good traction if we can get in front of people yeah, but out of sight out of mind. I think probably an accurate view at the moment.'*

Despite perceived issues with the cyber-security culture of the organisation, for example, cyber security being low on people's priorities, the elite interviews did express hope that the culture was changing for the better.

EI2: *'We're getting there we're getting there we're definitely say we're definitely better at communicating the better people coming forward to us yeah.'*

EI1: *'we're hoping all these kinds of different actions are slowly changing the culture.'*

Moreover, EI1 and EI2 described how they aimed to improve their security culture through security awareness methods and cultural assessments with outside vendors and academics, such as the current research. EI1 and EI2 also stated that such notions of building a better security culture were supported by the board and were in that way supported from the top down.

EI1: *'they* [the board] *want us to recruit they want us to kind of build up our resilience to the firm…'*

EI2: *'…it's getting cascaded down, from the board down, the support that they're showing, which is appreciated.'*

Overall, this theme demonstrated that participants generally, on a surface level, thought of their cyber-security culture within the organisation as good. The other themes throughout this findings' sections aim to shed more light on further details of cultural and social aspects

beyond descriptions of 'good'. However, the surface-level descriptions discussed in this subtheme are still valuable findings. The descriptions demonstrate the extent to which participants have given thought to culture within the firm and their thoughts on whether the culture was overall positive or negative. The elite interviews demonstrated the view that cyber security was not at the forefront of people's minds, which is not necessarily contradictory to the interview and focus group view of employees but does display a slightly more negative narrative.

4.3 Responsibility: 'It's managed for us'

An organisation consists of its employees, their roles, and their interactions with one another. Each member has a set of responsibilities, generally set out to them by their employer in a contract or developed through a mutual understanding in a psychological contract. As discussed, preserving cyber security is a clear goal of the current organisation, as it is with most organisations. The participant's ideas surrounding responsibility came out as a clear theme through the data. The meaning of responsibility in this context refers to the participant's feelings and perceptions towards whom they felt were accountable for the firm's cyber security.

Most participants who referenced responsibility felt that cyber security was not their individual responsibility, or at least not solely their own. This emerged from the data in a few of the participant interviews in some form of paraphrase of *'it's managed for us',* managed *'in the background,* or *'it's taken care of'.* This finding demonstrates that many participants believed the cyber security of the firm to be taken care of by a certain team behind closed doors, but also suggests an element of trust in the cyber-security team that they were capable of doing this for the organisation. It also insinuates that, although participants believed cyber security to be *'taken care of,'* employees did not necessarily understand or have knowledge of how this was being done.

> G1P6: *'I think they kind of just operate in the background so that everything feels this as usual for us, but they're in the background making sure that it's secure.'*

> G1P5: *'feel that that is just taken care of I know I know it sounds very trusting of people but I think a lot of it is to do with the fact that we're very very large law firm and like I said before you just expect that even if you don't hear anything that there's somebody somewhere magically taking care of things.'*

Some participants also stressed that the cyber security's team responsibility was not just technological but also stated that the cyber-security team had a duty to make sure that they, as employees, were cyber security 'aware' and trained to an 'acceptable' degree. Acceptable here refers to having the knowledge and ability to act and behave in a secure manner, as viewed by the cyber-security team. This then puts the responsibility for how employees behave on their training, which can then again be traced back to the cyber-security team.

The statements *'it's managed for us,'* and similar were often a reference to cyber security being managed in cyber security or 'IT' as some participants referred to it as. Referencing cyber security as IT might be a wider example of confusion between the two functions. The two terms were used interchangeably by some participants, without much evidence of knowledge that the two were separate with two different functions, as was the case within the organisation. This lack of knowledge could hinder participants' ability to speak to the right people if a cyber-security incident was to occur. Moreover, it was stated in the elite interviews that the security awareness specialists within the information security team wanted to be seen as *'engaging trusted advisors'* rather than the *'IT police'* (EI1). Hence, the fact participants mislabelled the information security team serves as an example of this separation and responsibility not being clear to or understood by employees. Other more broadly suggested it was the organisation's responsibility and did not specify an individual or a department. However, it is also possible that references to 'the organisation' were referring to management or the cyber-security department and policy makers of cyber security.

A few participants argued that seeing cyber security as the cyber security team's responsibility was due to functionality in the way the business was set up to run, in that people were given job roles and would do work pertaining to this role.

> G2P2: *'I would expect it to be their role, they're all because they're the experts, it's the same as project management, right?'*

This was said to be particularly akin to working within a law firm, where there is a fee earning side and a business side of the firm. It is seen as important, therefore, that if *'you're a fee earning lawyer you should be doing fee earning work'* (G2P8). This argument makes a case for a separation of responsibility between different job functions. This is because, otherwise, lawyers would spend time doing work that would not be directly bringing in money for the organisation, such as cyber-security policy. On the other hand, those on the organisation's business side do not have billable hours and so are not bringing in money directly by the hour. Lawyers should not, therefore, by this way of thinking, have to spend time discerning cyber-security policies, nor should policies create inconveniences and reduce productivity in the lawyers' work.

Participants felt that it was beneficial that cyber security was dealt with in the backgound. It helped them focus on their job role, while the designated teams were focussed on keeping the firm secure by evidence based technological safeguarding and training employees when needed.

> G2P7: *'…that's the benefit you don't want to be constantly thinking, oh well is this secure, is this secure and then having to kind of retrace your steps and back everything decide on basis of risk you'd like to have that done for you so that you can concentrate on what your actual job role is, you know, I wouldn't want many lawyers to be constantly worried about these things…'*

A few others described responsibility in terms of attributability, the degree to which something going wrong with cyber security inside the firm, such as a cyber-attack, was the organisation's responsibility, the cyber-security team's responsibility, or the individual who caused the cyber-security breach. This is an important distinction, as although employees may take responsibility for small actions they take throughout the day, this may be different to taking responsibility for a cyber-attack that came about because of a misplaced password, for example. Most argued that it was the responsibility of the organisation, the cyber-security

team, or a combination/shared responsibility, but that no individual employee should be the one *'taking the fall'* if something was to go wrong and a breach was to happen.

> G1P4: *'…the information security have a stricter approach to information security implementation at the firm which I understand because they are the ones who are responsible for and in charge of all the information assets and if that is a hack or a breach or anything of that sort then they will be the ones who will be in the firing line'*

This is substantiated by the previous finding within this section on responsibility, where it was shown that participants also saw the cyber-security team as responsible for their training and awareness. Participants did not see it as reasonable to be imputed for any breaches in the firm's cyber-security systems by the cyber-security team when this same team had trained them.

Some participants added the caveat that unless an individual had been particularly reckless or had not taken basic precautions, the onus should not be on the individual. However, if the said individual had done something distinctly wrong, then the individual was responsible. Others proposed it was the individual's responsibility 'to a point', suggesting that although individuals play a part in taking responsibility for cyber security and the volume of, for example, email traffic employees deal with makes cyber security difficult to manage for the individual employee.

> FG4P8: *'obviously that person should be kind of aware of it and on the ball but then also they should really be with like this many employees and stuff in a company there probably should be like safeguards and places as well.'*

> FG6P13: *'I think that there is responsibility on the individual that if they haven't taken the correct precautions and something like that's happened but. I suppose the same time the firm should be doing everything in terms of not allowing those things to come through on servers or whatever and then also has the responsibility of dealing with it after it's happened.'*

A few others also suggested that individuals did have a 'duty to be compliant'. However, the data shows that ultimate responsibility for cyber security and any potential breaches was perceived to remain with the organisation and the cyber-security team more specifically.

One participant from the elite interviews stated that they would like to see employees taking responsibility for their actions and that this was extremely important for the firm. For instance, if an employee spots a phishing email and reports it before anyone else in the business has clicked on it, they would like to see them rewarded or use their success to demonstrate good cyber-security behaviour to others.

> EI1: *'I really do want to empower people to a take responsibility for their actions and be kind and be kind of make them heroes for the business'*

This finding suggests that the cyber-security staff want employees in the organisation to take more responsibility for their behaviours in order to make them part of the solution to cyber-security issues.

In summary, this subtheme demonstrated that participants saw the cyber-security team as responsible for managing, in the background, cyber security for the general benefit of employees, especially in some cases, the lawyers or fee earning side. This will be described further in section 4.5 of this chapter. Moreover, participants thought that the cyber-security team, or the central 'organisation' should be the ones to take responsibility if a cyber-security incident were to occur.

4.4 Separate but Accessible: How the Cyber-Security Team Functions

The previous theme captured data surrounding how participants perceived the responsibility of cyber security and demonstrated that cyber security was seen as managed for the employees by the organisation or the specific cyber-security team. This also speaks to the data surrounding how participants viewed the cyber-security team and broader cyber security in general to function within the organisation.

A few participants expressed that the cyber-security team and the work they did were considered separate from the participant's individual job roles, with some expressing an 'us' and 'them' attitude or, similar to the previous responsibility theme, that the cyber-security team stayed mainly in the background. However, this was viewed as a positive, as participants did not want cyber security to be domineering.

> G1P6: *'They kind of stay in the background, we only really hear from them if they've detected something that they really want us to be aware of and I think that's a good thing yeah. I think they were if there were two overbearing we'd just feel very stifled.'*

Moreover, despite the mentions of cyber security not being constantly visible directly to employees, participants often mentioned that they felt supported, safe or secure within the organisation and were able to receive help when they needed it. This demonstrates that although cyber security is seen to function in the background, employees view it as accessible.

> FG2P3: *'they're very good at coming back promptly, so I feel I've got support in those situations where I'm I may have some doubt as to whether or not something is safe.'*

Furthermore, if participants described their view on the cyber-security team, many participants confused the terms cyber security and IT by using them interchangeably as if they were the same department and same employees with the same function. By doing so, the data suggests that participants see the two as having the same function.

> G1P1: *'I come back to what I touched on before, a lot of the people who like say from the employee side will look at the IT like it's the IT's job to make sure it's secure.'*

This sentiment was echoed by the elite interviews, where it was expressed that they believed employees to view cyber security as part of IT.

EI1: *'a lot of us lots of people still see it as IT risk, or kind of closely embedded with IT, so there's a kind of an educational piece around who we are.'*

However, participants also mentioned that they felt there was a two-way dialogue between the cyber-security team and the wider firm. Participants felt they could give feedback and were often asked for feedback by the firm or cyber-security team. This was seen as generally encouraged by the firm and, therefore, perhaps related to the broader context rather than specifically related to cyber security. For example, one participant mentioned that there had previously been a competition set up for people to develop policy suggestions and improvements across the firm. Others mentioned that the cyber-security team often reminded employees to contact the team if they had any questions or concerns pertaining to cyber security. This demonstrates that employees had clear examples of having contact and being able to give feedback to the cyber-security team. However, it was unclear how often or whether participants took advantage of this communication channel, even if feedback on policies within the wider organisational context was encouraged.

G1P8: *'I mean, we do we get emails from the kind of central spirit* cyber-security *team and fairly regularly just kind of reminding those on things like phishing and things like that. And they do always say if you have any questions or and any queries about policies that you can get in touch with them, so I would know if you for that kind of query or to give feedback on that kind of thing.'*

However, the direct feedback to cyber security did seem to depend on job function, with departments who had the closest contact or crossed over with cyber security giving the most feedback. Others understood that subject matter experts within the firm would often be called upon if there was a knowledge gap.

Participants who mentioned there was little opportunity for feedback expressed the idea that being able to give feedback to the cyber-security team directly on policies and issues that they might be experiencing would be a useful exercise. However, they did not expressly give direction on how this could be done.

Overall, this theme demonstrated data from participants who expressed that the cyber-security team and their work were often considered separate from the participants' job roles, with some expressing an 'us' and 'them' attitude. A few participants mentioned that they felt feedback within the organisation on their policies was encouraged.

4.5 Lawyers are Different: Cultural Differences in Cyber Security

The most noticeable cultural difference in the data highlighted a difference between the firm's lawyers and the firm's business side. Participants on the business side of the firm, often expressed that fee earners generally paid less attention to or had less time to pay attention to cyber security and the policies surrounding this. Participants said that the fee earner's view was that partaking in cyber-security training and similar initiatives were not billable, and so fee earners generally showed less tolerance for such training or any policies that might slow down their billable client facing work. Participants generally reasoned this notion by saying that the fee earners top priority and responsibility was to make the firm money, and that the attitude of putting the client first is one that *'is correct as well because client satisfaction matters a lot*' (G1P4).

> G2P3: *'Yeah endless and every time you make a change there's pushback in some way or other even to really simple things'*
>
> G1P7: *'Yeah because of these campaigns people often won't think as I said, you're not going to think about it as a fee earner, and it's probably the last thing on your mind.'*
>
> G2P8: *'I think of the way the business is set up is, you're a fee earning lawyer you should be doing fee earning work.'*

In some cases, participants mentioned that they believed this to mean fee earners were more likely to push back on particular policies or even attempt to circumvent certain controls.

Those participants who worked in risk or cyber security further stated that they received particular pushback on policies from lawyers if the policies were seen to extend the time of completing a task or complicate a task. For example, one participant gave an example relating to emails whereby a new feature was installed that would flag whether an email was coming from an internal or external source. However, the feature meant it was no longer possible to see an email in a preview on phones, which was considered a usability pain point. Employees would now have to click on the email to see its contents. This led to pushback from the fee earning side of the business and an eventual change to the policy.

> G1P3: *'It's most likely lawyers but it's not because they're always it's more just the fact that they need something and this is how they told to get it yeah and they haven't considered or don't really care what our security is saying so we have to find other ways around it.'*

Fee earners were also interviewed or participated in focus groups – although these interviews were less than those gathered from the business side, likely because they would have to take fee earning time out of their day to join the interview. Some lawyers highlighted that although their focus was on the client and fee earning, they still paid attention to security needs, but this was not their focus.

> G2P5: *'All of our work, can be billed to a clients and so I guess it means I can't… the driver is to do work and we're incentivized to do more and more work for clients because you have to bill certain number of hours a day so when I say it's a distraction from information security doesn't mean that I'm not conscious of and taking my work for clients, but what I mean is that I can't spend seven hours a day helping my organisation with this information security because if I did that, it would on paper as if I did not do any work that day.'*

In addition, a few participants also noted a possible hierarchal split between senior and junior employees. Most participants who mentioned this suggested that more senior employees, such as partners in the firm (in this particular firm, there were hundreds), had less time to be

concerned with cyber security – similarly to fee earners and lawyers. For example, it was argued by one participant that the more senior one got, the more emails an employee might get, which meant it would be easier to overlook something suspicious. Participants mentioned it was often harder to get these more senior partners to comply with cyber-security policies, sign off on annual declarations and watch cyber-security training videos. Others suggested an alternative reason for poorer cyber-security behaviours in more senior employees; the idea that younger generations were more technologically able, *'I think those are of a younger age probably more aware and tech savvy'* (G2P9).

> G2P1: *'It varies, it varies on role, the more senior they are sometimes you find the less they seem to care about the actual policies and stuff like that.'*

However, the view that senior employees were less interested in cyber security than junior employees was not unanimous when participants spoke about a hierarchal split. Some participants thought that junior and senior employees behave similarly.

In terms of cultural differences between employees and different fractions of the organisation, EI1 and EI2 mentioned that some employees and managers were more onboard with cyber-security training than others but did not specify categories. However, they also stated that they were directing cyber-security messages and training to people based on their specific roles, and in this way, further substantiating the notion that cyber security needs to be taught differently depending on attributes of the employee, such as job role.

> EI1: *'So this is the advisory and support side of our function and their coming to us asking for stuff and we're just happy that they want to engage with us. Others, very well they just disregard what we're trying to do, and unless it comes down from the board or the exec, they'll quite happily let it go.'*

> EI1: *'making it* [security messaging and training] *more relevant to their roles rather than this one-size-fits-all so we're hoping all these kind of different actions are slowly changing the culture'*

Overall, this subtheme demonstrates that participants see the fee earning side of the firm to be less compliant in cyber security than the business side, or at least that they have less time to think about security. Some participants perceived this to be understandable, as the fee earners brought in revenue for the business. The lawyers also explained that it was not feasible or productive for them to spend much time on cyber security. This difference was similar to a smaller difference in culture between more senior and more junior staff.

4.6 Law Firms are Different: Cultural Differences in Cyber Security

In juxtaposition to the finding in the previous subsection, participants also perceived the nature of working for a law firm to mean that the cyber-security awareness was higher among employees on both the business and fee earning sides of the firm than it would be in other types of business. Participants argued that, in a law firm, employees were often trained in legal privilege and confidentiality extensively as part of their onboarding. Participants saw legal privilege and confidentiality as relating very closely to cyber security and that this previous knowledge meant that they had greater competency in cyber security. For example, some participants mentioned that they were trained in confidentiality and data handling, which was described as being related to cyber security and privacy. Such training was said to occur every 6 to 12 months, in addition to any cyber security-specific training. In the participants' view, this meant the firm had very stringent rules for employees to follow regarding confidentiality.

> G1P5: *'I suppose there is that side of it too that you know you working in the law firm maybe if someone was working in a sweet factory and they had ingredients for I don't know lollipops, they might think they could share it with someone else but I think when it's a law firm, maybe that's one reason why you've kind of a more conscious of security…'*

Furthermore, they had to sign NDAs with clients and other lawyers extensively, owing to the nature of their work. Some participants explored the idea that because many employees had

previously studied law, this predisposed them to *'good at adhering to compliance and rules'* (G2P2). This was supported by the mentioned fact that lawyers could lose their licence to practice law and face legal charges if they were to share certain privileged information with anyone.

> G1P6*: '…they deal with a concept of legal privilege. It just means you are not legally allowed to share this information with anybody. It's against the law you could lose your license to practice law. So I think lawyers themselves are very very aware of Information security and the managers of younger lawyers will really impress upon them you cannot share this…'*

As the quote above demonstrates, employees saw the legality of legal privilege, which entitles a party to withhold evidence from production to a third party or the court, to be relevant or similar to cyber security. This was presumably because both ideas concern the security of data or information. It was impressed upon the researcher that the nature of law meant it was necessary not to leave confidential information lying around and available for others to read. Others suggested that on top of the training they received and the policies they imposed in-house, the clients they worked with also imposed their own sets of confidentiality and security policies, increasing the presence of security measures in their day-to-day activities.

> G2P1: *'You know, our clients will stipulate sometimes quite stringent security controls, we have clients across multiple sectors, you know, financial services, you know, they tend to have quite elaborate and complicated security requirements.'*

> G2P2: *'…the projects I work with just put has put me in that mental like as I say that mental it gives me that mental attitude or not attitude that's on the right word, but like it puts me in that mindset of security.'*

In addition to the finding that law firms were perceived to have a good cyber-security mindset and more stringent policies than other industries, there were a few other perceived cultural differences. For example, a few participants saw a difference in cyber-security

behaviours depending on age, and one saw a difference between certain departments. However, these ideas did not aggregate from a great number of participants or quotes. However, this is important to note in the data as it adds to the idea that many participants perceived some form of cultural differences between employees one way or another – even if the cultural differences perceived had a few individual differences.

Moreover, EI1 and EI2 noted that this difference in cyber-security behaviours and culture changed by country, demonstrating that geography also impacts cyber-security culture. It is possible that this was not found in the interview and focus group data as all the interviews and focus groups were UK based.

> EI2: *'That's where you can see it certainly in Asia pack and Australia is renowned for you know, it's renowned for treating things completely different.'*

This subtheme largely demonstrates that employees perceived law as a profession where cyber-security values were heightened due to their similarity to law-related concepts, such as client confidentiality. This led participants to believe that people working in the law sector, or who had a background in law, had a heightened awareness of cyber security related issues and concepts and may behave more securely.

4.7 Summary of Findings

This theme brought together data in the form of subthemes that pertained to 'organisational perceptions of security culture'. This data relates to the social aspects of cyber security within organisations, rather than the individual cognitive perceptions, such as the social norms, social descriptions, and shared experiences of employees (McAlaney et al., 2016), for example, beliefs surrounding the culture of an organisation and how the cyber security team functions and is viewed. The data demonstrated that participants generally understood or saw the organisation's security culture to be good and strong, although they did not provide specific examples to support this. Participants further saw information to be managed for them by the cyber-security team, and some demonstrated an 'us' versus them mentality

when it came to this team but saw the team as accessible. Participants also highlighted a few cultural differences internally between employees and externally between sectors. Participants saw a difference between the fee earning and support staff sides of the business in terms of cyber-security behaviours, with fee earners having less time to think about cyber security. There was also a perceived difference between law firms and other sectors, with the argument that law firms were inherently different to other types of organisations as they were trained in related concepts.

4.8 Discussion

This discussion synthesises and grounds the findings from this chapter within the research and theory from the literature review section. This discussion explores why certain perceptions might exist by utilising insights from research on psychological theories and usable security research surrounding cyber-security culture (Da Veiga, 2015; Durojaiye et al., 2020; Glaspie & Karwowski, 2017; Ruighaver et al., 2007; Uchendu et al., 2021). Hence, producing insights into how cyber-security culture and other social aspects of cyber security are viewed and function on an everyday level contextually within an organisation. The findings from this theme have a range of important implications and may assist in giving insight for future developments in cyber-security culture research, as well as insight for industry. Three psychological theories, namely PMT (Prentice-Dunn & Rogers, 1986), the EPPM (Witte, 1996) and the TPB (Ajzen, 1985), will be used to deepen insights from the findings by providing a theoretical lens through which to make sense of the data.

4.8.1 Usable Security Scholarship

The findings demonstrated how the participants in the current study viewed their security culture holistically. Much of the previous literature measures or presents instruments to evaluate security culture through surveys or behavioural measures, ultimately ending with a decision to help organisations decide whether their security culture is ‘good’ or ‘bad’ (Da Veiga & Martins, 2015; Glaspie & Karwowski, 2017; Ruighaver et al., 2007). In such studies, a

‘good’ or ‘positive’ cyber-security culture would ideally involve seeing that employees adhere to security policies (Glaspie & Karwowski, 2017; Ruighaver et al., 2007). A ‘bad’ or ‘negative’ cyber-security culture then may encompass a lack of understanding of cyber security and compliance with security measures. Usable security scholars suggest that organisations should not expect to have a ‘good’ cyber-security culture without usable policies and without listening to what works for users. Therefore, 'good' should be an attainable goal (Sasse & Rashid, 2021).

The researcher took a different approach in the current research and asked participants to describe their organisation's culture. Participants displayed confidence in their belief that the security culture in the firm was good and strong but arguably could not find solid reasoning for this belief. However, it is possible that the concept of security culture, or at least the term, was new to participants and that the reasoning came out in the other subthemes seen in this chapter. For example, participants’ views of cultural differences between employees added further nuances. The elite interviews supported the view of a good security culture, who argued that although cyber security was slightly ‘out of sight out of mind’, the culture was changing for the better and that the organisation was ahead of other firms. However, the extent to which the elite interviews would state that the cyber-security culture of the organisation is bad should be questioned. It is possible that the elite interviewees were motivated to paint the organisation's cyber-security culture positively.

The current research presents a new deeper way of looking at culture by directly interviewing and asking employees rather than surveying culture through questionnaires (Da Veiga & Eloff, 2010; Rantos et al., 2012). Rather than answering predetermined questions, often with pre-set Likert scale answers, as is the case in many cultural surveys (Georgiadou et al., 2021), interviews and focus groups allow participants to freely describe their culture, offering insights that may not have otherwise been gathered. Moreover, interviews and focus groups are, in some ways, less driven by the researchers’ thoughts on what security culture means. Surveys rely on previously defined components, whereas although interviews and focus groups have topic guides, participants can input their thoughts and direct the conversation.

The ‘good’ perceptions of security culture are perhaps related to findings within previous literature which have looked at what might encourage such a culture. For example, previous literature finds top management support for cyber security to be important for developing a strong cyber-security culture (Uchendu et al., 2021). In the current research, the elite interviewees stated they had support from the board for their cyber-security strategies and that the security team appreciated this. This lends support to Uchendu et al. (2021), who found that top management support, especially that relating to security policy and cyber-security awareness and training, was a key factor when organisations build and develop cyber-security cultures. We argue, therefore, that top-management support could be one of the reasons for the employee’s belief that their cyber-security culture was good and strong. Moreover, the study demonstrates this finding in a contextually aware environment. The current research arguably, therefore, further stresses the importance of top management and board-level support in the development of cyber-security culture, adding to previous literature (Ashenden & Sasse, 2013; Hu et al., 2012; Uchendu et al., 2021). The reasons for belief in the firm's good and strong security culture could also be related to the other subthemes of this chapter. Of course, security culture is such a wide concept that other findings in the other themes of the current research may also be influencing factors, but this will be discussed in the overall meta-discussion section.

Participants in the current study also noted cyber security-related cultural differences or subcultures between members of the organisation and between their organisation and other organisations. This general trend of differing cultures within and between organisations has been consistent in the wider literature on cyber-security cultures (Da Veiga, 2016; Da Veiga & Martins, 2017; Hofstede, 1998; Kolkowska, 2011; Muendo, 2014; Whelan, 2017). For example, researchers have found cultural differences in cyber-security behaviour between managers and users (Albrechtsen & Hovden, 2009; Balozian et al., 2019), IT and non-IT staff, and between individuals in different geographical locations (Da Veiga & Martins, 2015). In the current organisation, ideas of cultural difference centred around the ideas that firstly, there was a divide between the fee earning side of the organisation and the business side, and secondly, that a perception that the current law firm was ‘better’ than others.

In the current research, participants perceived that fee earners generally showed less tolerance towards cyber-security policies compared to support staff, as time spent on cyber security was not billable. While differences in cyber-security culture between departments are corroborated in relatable research (Albrechtsen & Hovden, 2009; Da Veiga, 2016; Da Veiga & Martins, 2017; Hofstede, 1998; Kolkowska, 2011; Muendo, 2014; Whelan, 2017), at time of writing, there has not been any specific cyber-security research looking at the differences between fee earning and business sides of organisations. Many sectors have organisations with these two business components beyond law firms, such as financial institutions and consultancies. Forstenlechner et al. (2009) found that the key narrative felt by support staff within a law firm was that "You are either a fee earner or a fee burner" and that this mentality often leads to reduced working morale in such staff. This demonstrates that although there has been no research directly related to cyber security, a perception of a split between staff resides in law firms. Therefore, the current findings add to this narrative by demonstrating a difference in cyber security between fee earners and support staff. This is important as it reflects how organisational structures can impact culture and that there is not just one uniform 'cyber-security culture' in an organisation. This is important for researchers and industry professionals developing cyber-security training, as training will also need to reflect these nuances and assist individuals in different ways.

The belief that law firms are different, namely better, in aspects of cyber-security culture was also a core belief among participants. Participants stated their reasons for this view were because the study of law, and the concepts within the study, were related to concepts of cyber security, such as data protection. However, not all employees within law firms studied law, though the participants might argue that everyone in law firms must comply with strict data regulation and legal privilege laws and so, in this way, are knowledgeable of the area. Heikkila (2009) argues that law firms store and maintain highly confidential data, such as attorney-client privileged information, financials, trade secrets, intellectual properties, and other sensitive information. There is, therefore, a codified ethical obligation to protect law firm client data from unauthorised access. It is therefore made known to employees, through cyber-security policies, that security breaches are known to jeopardise the reputation of the law firm and could have a substantial financial impact (Heikkila., 2009). The maintenance and storage of data in law firms may influence cyber-security awareness policy (Heikkila., 2009).

This suggests that law firms are, through policies, more aware of policy than other firms that do not have the same stringent requirements. However, as discussed in the literature review, awareness does not always lead to good behaviour or a strong security culture (Bada et al., 2019). Moreover, it is possible that holding the belief that your organisation is better than others is an example of an optimism bias. The findings of the optimism bias will be discussed in more detail in chapter 6.

There was a belief among employees that the cyber-security team should take the main responsibility for cyber security within the firm and that the team were in the background making the organisation secure. Moreover, the team was viewed as separate from the rest of the organisation in some ways. This aligns with the literature looking at the impact of perceptions of responsibility on compliance. The literature often argues that high levels of responsibility are a precursor to high levels of compliance (Filipczuk et al., 2019; Hadlington, 2018; Kim & Han, 2019). However, as the findings demonstrate and will continue to demonstrate as we move through the remaining findings chapters, there does not seem to be a report of a high level of compliance issues within the current organisation. On the other hand, when compliance issues were highlighted, these were generally spoken about in relation to certain areas of the organisation, such as fee earners. Participants argued that fee earners had a larger corporate responsibility to earn money and, therefore, should perhaps have less responsibility towards everyday cyber-security issues. Put together, the findings from previous research (Filipczuk et al., 2019; Hadlington, 2018; Kim & Han, 2019) and those from the theme in the current chapter might give insight into why compliance is lower among fee earners if they have a larger overriding responsibility to earn money for the firm.

Moreover, one of the elite interviewees mentioned wanting employees to take more responsibility. This discrepancy between the views of cyber-security professionals and non-cyber security employees is not new in the literature. Research has demonstrated that there are many points of divergence between the perspectives of ordinary organisational insiders and cyber-security professionals (Posey et al., 2014). For example, research demonstrates dissimilarities in views between the two groups on topics such as what increases employee's self-efficacy, response efficacy and threat severity and what is considered an adaptive response (Posey et al., 2014; Posey et al., 2011), with employees often finding security topics

dull and confusing (Haney & Lutters, 2018). Moreover, much research concerning the behaviours and thoughts of employees, such as perceptions of responsibility, has often been accumulated from the opinions and experiences of cyber-security professionals (Haney & Lutters, 2018; Loch et al., 1992; Whitman, 2003). Hence, the current research corroborates these findings by demonstrating that ideas surrounding responsibility can differ between cyber-security staff and other employees within an organisation.

The degree to which employees should take responsibility for everyday cyber security within organisations is contentious. In the current findings, some employees did show a degree of responsibility, referenced by quotes stating that employees were responsible for taking precautions and being aware, but that there should be safeguards in place as well. This finding confirms previous studies that have demonstrated employees feel responsible for their organisations' information resources by acting in a precautionary way (Posey et al., 2014). However, they also feel that all other protections possible should be in place and be the main protecting factor. A key takeaway from previous research then is to ensure that communication to employees includes the clear message that security is everybody's job (Posey et al., 2014), at least to an extent. The current findings substantiate this notion by demonstrating that employees can feel a sense of responsibility without feeling the burden too much and whilst feeling as though they are made safe by the cyber-security team.

Participants in the current study also appreciated the ability to feedback to the cyber-security department and felt able to raise any issues or concerns. This would have seemingly added to a feeling of support in terms of cyber security. This fits in with research that recommends cyber-security professionals use tools that facilitate systematic feedback from users/employees (Reinfelder et al.,2019) in aid of including employees and the human factor in the cyber-security process (Acar et al., 2016; Green & Smith, 2016). The current research adds to this dialogue in the literature by demonstrating that employees find this to be a useful exercise that they appreciate. Moreover, in the current study, participants also expressed wanting more opportunities for feedback on specific policies. This fits into usable security research (Inglesant & Sasse, 2010; Kirlappos & Sasse, 2014) by demonstrating that employees feel it would be useful to give feedback on policies, which would seemingly improve their usability. Additionally, user experience research, a field of human-computer

interaction that attempts to understand how humans experience and interact with technology (Glanznig, 2012), is growing and has shown to be greatly useful. There is seemingly no reason why user experience research cannot be applied to, and improve, the cyber-security field.

4.8.2 Psychological Models

As predictors of behaviour, PMT (Prentice-Dunn & Rogers, 1986), EPPM (Witte, 1992) and TPB (Ajzen, 1985) models might offer ideas and deepen insights surrounding the idea of cyber-security culture within the current findings. While PMT offers explanations as to why people engage in unhealthy practices, such as those of a cyber-security nature, and offers suggestions for changing those behaviours (Prentice-Dunn & Rogers, 1986), it can also help us understand why participants within the current study broadly reference their security culture to be good, and whether this is beneficial. This application of PMT adds to previous research looking at the use of PMT to understand employees in cyber security, where the existence of PMT components has been found (Blythe et al., 2015; Herath & Rao, 2009; Williams et al., 2019a; Williams et al., 2019b). Employees in the current study expressed confidence that they were part of a good cyber-security culture. This belief might represent feelings of high self-efficacy and high response efficacy. In PMT, high efficacy levels increase the likelihood of individuals performing an adaptive behaviour (Prentice-Dunn & Rogers, 1986). Hence, the positive perceptions held by participants in the current study surrounding the organisation's cyber-security culture may, in turn, improve cyber-security behaviours. Research demonstrates that increased detection efficacy with phishing emails increases scoping adaptiveness, increasing detection effort and accuracy (Wang, Li, & Rao, 2017).

Other pieces of research have also demonstrated that individuals who have confidence in their self-ability and security knowledge seem to be more competent in dealing with cyber threats (Albladi & Weir, 2020; Flores et al., 2015; Wright & Marett, 2010). Confidence is a concept related to and correlated with self-efficacy. In some cases, researchers may refer to self-efficacy as confidence in one's own ability to execute protective behaviours (Van Der Roest et al., 2017). Hence, confidence in one's abilities to protect oneself may increase the

detection of phishing emails and competency to deal with threats in some circumstances. This demonstrates that these individuals' positive security beliefs may be beneficial somehow. One could also argue that the positive beliefs held by participants in the current study surrounding cyber-security culture could be a form of the optimism bias, especially given that participants did not give specific reasons to support this belief. The latter could lend evidence to the notion that the participants' thoughts of a good culture were largely baseless. However, a false belief that one's culture is good would not necessarily lead to unintentional negative consequences. As demonstrated in the previous paragraph, confidence can lead to competency rather than just skill and awareness (Albladi & Weir, 2020; Flores et al., 2015; Wang et al., 2017; Wright & Marett, 2010).

The EPPM (Witte, 1992), as a model largely based on PMT, offers similar insights to PMT in this instance. The EPPM also posits that high efficacy levels lead to an increased likelihood of behaving in adaptive ways towards threats (Witte, 1992) if the perceived threat level is not so high as to negate this. This may, in turn, improve cyber-security behaviours. However, the EPPM also theorises that for a person to feel motivated enough to begin weighing up the efficacy of the recommended response with the perceived strength and severity of the communicated threat, they must first additively appraise how severe the threat appears to be and their personal vulnerability to it. Only if perceptions of the threat severity and vulnerability reach a particularly increased level, will individuals begin to weigh up efficacy (Witte, 1992). This supports previous experiments and surveys demonstrating the use of the EPPM model in understanding the influence of threat and efficacy on cyber-security behaviour (Chen et al., 2021; Masuch et al., 2021; Zhang & Borden, 2020). Unlike such experimental studies, in the current findings, it would be hard to make a definitive judgment about whether participants were actively going through the different appraisal processes in this model. Nevertheless, we can see how increased efficacy, represented by participants' positive views of the organisation's cyber-security culture, could benefit employees and the wider firm (Albladi & Weir, 2020; Flores et al., 2015; Wright & Marett, 2010). Hence, the current research validates previous experimental work by showing possible manifestations of the model in a real-life context. Moreover, this data in the current findings do not lend additional support to PMT or the EPPM but demonstrates possible attributes of the model reflected in cyber-security perceptions and behaviour within the organisation.

The TPB (Ajzen, 1985) model may also deepen insights surrounding the idea of cyber-security culture within the current findings. As discussed in the literature review, TPB proposes that the intention to perform a specific behaviour can be predicted accurately by three considerations (Ajzen, 1985): behavioural beliefs, normative beliefs and control beliefs. In this way, such beliefs are related to cyber-security culture, as cyber-security culture represents a set of beliefs, behaviours, norms, and values developed and shared by colleagues towards cyber security (D'Arcy & Greene, 2014; Ertan et al., 2020). Normative beliefs refer to perceptions about the possible expectations of other individuals and one's motivation to fulfil these expectations (Ajzen, 1985). Therefore, in the current findings, the idea that security culture was collectively good could lead to the normative belief that 'good' behaviour is what is expected within the organisation, which would help explain the idea of a 'good' culture, as the 'norm' would be to comply with cyber-security policy. Moreover, a 'good' cyber-security culture may also include ideas surrounding behaviour and control (Ajzen, 1985) by producing positive personal attitudes towards cyber-security behaviour and high behavioural control through ability. The positive attitudes again might be represented in the findings by ideas that the culture is good and that most people were well behaved. The theory posits that the more favourable the attitude and subjective norm, and the better the perceived behavioural control, the greater the person's intention to perform a behaviour. Hence, the belief that cyber-security culture is good, in the eyes of TPB, leads to good cyber-security behaviour (Ajzen, 1985). Similar to other theories, this interpretation suggests that positive beliefs of one's own culture may be advantageous for the organisation and its employees. These findings demonstrate how TPB may be used to interpret employee behaviour and perceptions in this research.

Psychological theories may also offer insight into concepts relating to cyber-security responsibility. Through the lens of PMT (Prentice-Dunn & Rogers, 1986) and the EPPM (Witte, 1996), reduced responsibility could be a maladaptive thinking or defence strategy, whereby participants have a diminished sense of cyber-security responsibility owing to low levels of efficacy. This would mean that participants would be using, actively or not (Prentice-Dunn & Rogers, 1986), the idea of low responsibility to not take action to reduce threats. Therefore, individuals might defer cyber security action to those they believe in to have

greater responsibility for, and response efficacy over, the risk presented to them. For example, the cyber-security team. Researchers have previously asserted the belief that the responsibility of cyber security is the cyber-security team's is a maladaptive perception that encourages individuals to engage in non-protective responses (Posey et al., 2014). It should be reiterated that, as the findings demonstrate, there does not seem to be a high report of non-compliance issues within the current organisation or a significant lack of motivation to behave securely. Moreover, as we will see in Chapter 7, it is also possible that compliance issues may stem from usability issues relating to policies. The lack of high non-compliance rates suggests, through the lens of PMT or the EPPM, that it is possible that employees within the current study had healthy attitudes towards responsibility, as the attitudes have not seemingly led to non-protective behaviours. Apart from in a few mentioned cases of fee earners, where reduced responsibility is seemingly accepted due to the nature of work. However, the current research did not have access to data on 'actual' behaviours, so it is also possible that the participants were not aware of other employees circumventing policy or did not want to admit to 'bad' behaviour themselves.

4.8.3 Conclusions and Contributions

The previous section highlights where and how the current chapter's findings have supported, contributed to, and conflicted with previous empirical and theoretical work. The discussion of these findings first highlighted how the 'good' perceptions of security culture are perhaps related to findings within previous literature which have looked at what might encourage such a culture, and how top management support in the organisation is linked to this finding and supports findings within the literature (Ashenden & Sasse, 2013; Hu et al., 2012; Uchendu et al., 2021). Moreover, the current findings add to previous findings by demonstrating behavioural splits between groups within the organisation (Albrechtsen & Hovden, 2009; Da Veiga, 2016; Hofstede, 1998; Kolkowska, 2011; Muendo, 2014; Whelan, 2017), namely between fee earners and support staff. This split in cyber security between these types of staff, to our knowledge, is a new contribution and adds to Forstenlechner et al.'s (2009) findings regarding the divide in law firms between fee earners and support staff. The findings surrounding this split were also discussed in reference to research on

responsibility, suggesting that reduced cyber-security responsibility among fee earners could be why they are seen to behave less securely. Cyber-security responsibility was also discussed in reference to the PMT model and the degree to which employees should take responsibility. Research that recommends systematic feedback from users/employees was considered along with the present findings that employees want opportunities to give feedback (Reinfelder et al., 2019). Finally, the findings were discussed in terms of their relevance to PMT, EPPM and TPB. As described by PMT and EPPM, concepts of efficacy could be seen in the current findings, and the models' implications of this were discussed. The TPB was discussed in terms of how behavioural beliefs, normative beliefs and control beliefs might be relevant to views of security culture. The discussion of the models demonstrates how the previous survey-based and experimental work might be furthered by the findings of the concepts in qualitative context-driven research, another contribution of the current research.

Chapter 5. The Individual Human Element

5.1 Introduction

This chapter examines the theme of the individual human element. The individual human element refers to cognitive thinking patterns and personal views of different aspects of cyber security. This theme encompasses subthemes that emerged from the data as internal perceptions and biases and how employees are viewed in terms of the problemisation of cyber security, i.e., how the human element is viewed as a challenge for cyber security. Researchers have used this 'problemisation' approach in recent years to understand current conceptualisations in government and industry of cyber-security threats (Zimmermann & Renaud, 2019). As discussed in the literature review, previous research has demonstrated that the human is often viewed as a problem in cyber security (Goo et al., 2014; Hughes-Lartey et al., 2021; Lowry & Moody, 2015; Sabillon, 2022). This perceived 'problem' is then often dealt with by applying new security layers, training and policies that attempt to control humans and constrain their 'problematic' perceptions and behaviours (Sasse & Rashid, 2021; Zimmermann & Renaud, 2019). This then creates a narrative whereby all humans in a security system are treated at worst as malicious actors and, at best, ill-informed individuals, both of which can be counterproductive to security. Research similarly often points to 'faulty' or 'unhelpful' thinking processes in humans, which instead of accepting that humans often have innate or learnt biases towards perceptions of risks, set up security layers against them or try to change the behavioural outcomes (Hilbert, 2012; Vogt, 2019).

However, researchers have challenged this discourse by arguing that treating the human as a problem does not work, given that research has demonstrated that constraining and controlling individuals cause further cyber-security issues. Therefore, it is suggested that those in the cyber-security industry need to understand cyber security as a highly complex socio-technical issue where human mistakes co-emerge with technology (Vogt, 2019; Zimmermann & Renaud, 2019). This mindset acknowledges humans as well-intentioned individuals, capable of being part of the solution to cyber security in order to enhance positive human-based knowledge that might assist cyber security outcomes and advances in

the field (Corradini, 2020; Morgan et al., 2020; Parkin et al., 2010; Reinfelder et al., 2019; Sasse et al., 2001; Zimmermann & Renaud, 2019). This theme encompasses expressed views of how the human element is perceived within the organisation, as well as the possible perceptions and biases of employees and the perceived psychological and behavioural impact of the organisation's cyber-security attack in 2017. The subthemes look at the optimism bias, pessimistic beliefs, perceptual impacts of the 2017 cyber-attack and the perception of human factor verses other threats. This chapter will then end with a discussion section, where findings will be synthesised and grounded within the research and theory from the literature review section, such as PMT and research on the consequences of blaming the user.

5.2 The Optimism Bias

As discussed in the literature review, the optimism bias refers to the belief that an outcome will be more favourable than the reality of this outcome (Sharot, 2011). There are different types and definitions of the optimism bias. Unrealistic comparative optimism can be confirmed if a person believes their own risk to be lower than their peers. However, people can also be considered to be unrealistically optimistic if they predict that a future outcome for themselves will be more positive than that pointed to by an objective standard. This is what is known as unrealistic absolute optimism. However, cyber security, and the perceived knowledge people possess, the likelihood of falling victim to an attack, or the likelihood of companies falling victim to attacks, is highly subjective. These specific concepts are usually measured quantitatively in order to see differences between predicted and actual outcomes.

In this qualitative study, we saw the optimism bias emerge in the data as overly positive 'it would not happen to me' ideas, hence defining this theme as variations of the optimism bias and other self-serving biases. These perceptions were presented by a large majority of participants. These ideas are generally based on little presented evidence. For example, participants did not mention they were better trained than the average person or possessed greater skills. It should be noted that as this research is purely qualitative and interpretive, we cannot measure the perceived risk participants have against 'actual' risk, as this was not

in the scope of the project and nor is there a standardised way of doing so. Positive ideas about the likelihood of falling victim to or being involved in a cyber-attack were visible in the data. Participants generally expressed these views in terms of personal risk or risk in terms of organisational risk. We will look at each individually.

Firstly, and perhaps most pertinent for this case study, the data demonstrated that many participants expressed various ideations of the organisation being less at risk or less likely to fall victim to an attack, either generally or compared to other organisations or law firms. A few participants argued that this was because this organisation specifically emphasised the importance of cyber security, something they saw other organisations as not doing.

> G1P7: *'I think you're always going to have some non-compliance, but I think overall as a firm we're probably on the better side of some of the behaviours than some of the other firms I've worked for, we're definitely better.'*

Similarly, a few participants expressed the view that they themselves were not the primary targets within the firm. For example, one participant backed up this way of thinking by saying they found it easy to spot the phishing tests that the organisation sent around and that this demonstrated that they were more aware than others of such attack vectors and hence less likely to fall victim to such an attack. At the same time, another participant argued that their previous job had also focussed on the importance of being cyber secure in the workplace, and therefore this way of thinking was well ingrained in their mind.

> G1P3: *'I've seen the phishing emails that they've sent around and I find them easy to spot other people may not do…'*

Some participants also suggested that they were not high-profile enough to warrant being a target, and therefore were less likely to be targeted and fall victim to an attack. A few participants compared themselves to others and stated that they were less likely than the average person or general population to be the victim of a cyber-attack. This was supported by suggestions that the general public did not have good IT infrastructure, such as VPNs set up.

Several other participants did not reference themselves as having optimistic beliefs but expressed ideas that other employees in the firm did have such attitudes, or that such beliefs were a general mindset within the firm. The ideas that participants had of other people's mindsets usually centred around ideas of *'it'll never happen to me attitudes'* (FG7P15) or the idea that no one was out to hurt them.

> G2P1: *'there was a bit of mentality of we're all just lawyers everyone loves lawyers, why would anyone want to hurt us yeah'*

Others thought, owing to the nature of a law firm, the organisation was perhaps more likely to be a target of cyber-security 'attack', usually referenced as a phishing attack, but still less likely to actually fall victim to an attack. Some participants also referenced specific security measures the firm had taken to protect them against cyber-security threats, expressing faith that these measures were enough to reduce the likeliness of being the victim of an attack.

> FG1P4: *'I think maybe more likely to be targeted and then less likely to click on stuff because A) we do have a bad experience of it but B) probably more messaging and communication regarding it than the majority of businesses.'*

This also demonstrates positive thinking and trusting attitudes towards the business's messaging and communications. This quote also hints at the repercussions of the previous cyber-attack, which will be discussed as a standalone theme in the next section. Often, participants who did express ideas that the company was at risk from cyber-security threats, then went on to reason that this risk was actually reduced in their specific case because the cyber-security team was *'more conscious than maybe some other teams'* (G1P8).

The second aspect of optimistic beliefs or biases that people had were related more to their lives away from work. On a personal level, some participants expressed the idea that they personally, at home or in their private lives, were not likely to be the victim of a cyber-attack or less likely than others to fall victim to a cyber-attack. One participant argued that this was *'human nature to have this, not in my backyard thinking'* (FG1P1), whereas a few others

argued it was because they were highly aware of the risk themselves. Some participants argued that the 'general public' would be more vulnerable to cyber-security risks than they would themselves. For example, one participant stated that when they see people on the news who have been victims of cyber-attacks, they often wonder '*why they divulged personal details*' (FG2P3), but stated that these people must be less aware and hence more vulnerable than themselves.

> FG2P3: *'I'm alive to the risk, it's not something I tend to worry about a great deal. I do have personal email accounts which is flooded with emails on a daily basis, most of which I just ignore or delete, there are a few I read from trusted sources, beyond that I don't tend to use too many devices. I don't use social media a lot, so I don't feel that I'm particularly exposed.'*

As partially demonstrated by the above quote, participants gave a number of reasons as to why they were unlikely to be victims of a cyber-attack personally. Some of these reasons centred around the idea that they were more knowledgeable than most on cyber-security risks. Other participants reasoned that they ignored most emails they received if they were not from trusted sources or did not use social media. Hence, they presumably believed they could not be targeted through those specific attack vectors.

However, there was also an opposing view that was visible in the data. This was the idea, put forward by a few of the participants, that although they were not likely to fall victim to an attack at work (even though the organisation might be a high target), they would be at a high risk of falling victim to an attack in their home lives. Participants gave various reasons for this; some argued that their cyber-security behaviours were worse at home. For example, they did not use strong passwords or did not have a secure VPN to connect to. In contrast, others stated that the firm had better security measures in place or were just generally less careful at home compared to work.

> FG4P9: *'I would say the same I feel like in my personal life I've been more susceptible to attacks like the fake emails or that stuff but work not generally'*

FG6P14: *'I think less likely to happen from your firms email than it would at home yeah, yeah.'*

This then suggests that for some people, there was a split between how they viewed themselves in terms of their cyber security between the workplace and their home lives. In light of the mass move to work from home, participants also spoke about the impact of the pandemic on cyber security, demonstrating that this might have skewed the original perception of a difference between work and home, with there being a blurring between the two spaces. However, this will be discussed in more detail in a later findings chapter dedicated to the data that came out around the pandemic and working from home.

Overall, this subtheme demonstrated that many participants displayed optimistic thinking about the firm's likelihood or their own likelihood of falling victim to a cyber-attack. This demonstrates how individual thinking can influence feelings towards cyber security. Participants often supported these beliefs with statements surrounding the high-security measures the firm had in place. Or that people thought it would never actually happen to them. Some participants expressed beliefs that they were more at risk in their personal lives, and this often contrasted to their perceived risk when they were at work. Furthermore, participants compared themselves and the firm to others and other organisations, generally with the viewpoint that they, or the wider firm, were 'better' in a cyber security sense.

5.3 The 2017 Cyber-Attack Increased Awareness and Reduced Risk

This subtheme was the biggest theme that came out from the data related to the cyber-attack experienced by the firm in 2017. As discussed in Chapter 3, the NotPetya ransomware attack infected hundreds of thousands of computers across the organisation's platform, encrypted all affected files and requested a ransom in bitcoin to regain access or avoid threat of deletion (Financial Times, 2017). In the days following the attack, the organisation struggled to operate without systems like email, billing, payment and human resources. An example of how the attack impacted employees can be seen in the quote below.

FG3P7: *'I remember the day it happened, and I was basically camped out in in Leeds trying to bring systems back for best part of two months, yeah. Bless my wife, she forgot I existed.'*

However, as this subtheme indicates, many employees had an understanding that, in the long-term, the cyber-attack increased awareness and reduced risk.

Although specific to the cyber-attack experienced by the firm, this subtheme fits well with the previous subtheme of the optimism bias and self-serving biases. Perhaps, surprisingly, the 2017 cyber-attack seemed to be referenced as a reason to why the firm was at a reduced risk of a cyber-attack. This is because the 2017 cyber-attack was also used as an additional reason why participants believed the firm to be less likely to fall victim to another cyber-attack in comparison to other organisations. Less likely was sometimes used without a reference to other organisations. Other participants did compare the firm to other law firms or organisations in general.

The cyber-attack was referenced often by participants. Broadly, the cyber-attack was referenced as having a 'massive impact' on the firm. Generally, this impact was viewed as being lasting and positive for the firm in many ways. Participants argued that, because of the firm's cyber-security attack in 2017, they were now more secure as a firm and less likely to be the victim of another attack. Participants gave different reasons for this belief. Many participants argued that this was because the firm was now at the forefront of security, that their security team had put many layers of security in place since the attack, or that the wider firm became acutely knowledgeable of the threats from that point on. For example, one participant mentioned there had been changes to the way their servers and back-ups operate, and another mentioned they were more conscious of the risks and ahead of the game.

G2P2: *'I think the firm as a result of that attack is probably a lot more secure. And just in terms of how we bring in new technologies I know for sure like I work in the service delivery team where we're always constantly working on new technology and everyone is a lot more risk adverse'*

> FG5P10: *'because they've you know been they've been you know attacked in the past and I think their kind of ahead of the game and here's our old saying once bitten, twice shy, so and I like to think that they're, you know, more conscious of what of what can happen'*

This again hints at an element of trust in the cyber-security teams and the security of the systems that the firm has in place. Participants, as evidenced by these quotes, saw the firm to be *'ahead of the game'* in terms of security and were positive about the new policies in place. One participant stated that post the attack the cyber-security team had a *'presence now and it is built in the in the behaviours of the teams and the fee earners'* (G2P2).

EI1 also mentioned that a cyber-security awareness campaign was built off the back of the attack.

> EI1: *'But what I can say is on the back of that* [2017 cyber-attack] *there was a huge information security program built on that… kind of reviewing everything that happened then.'*

Some participants simply stated that another similar event was unlikely to happen again and that the event was a once in a lifetime occurrence. This type of thinking seemed to be to do with the likelihood of an event occurring twice and was generally not supported by other reasonings. However, a few participants referenced the firm's robust response as a reason it would not happen again.

> G1P9: '*Obviously even though we did have the attack and that was really bad, that is like, a once in a lifetime thing that happens to a company.'*

Furthermore, the data showed that the shared experience of this cyber-attack often left employees feeling as though it had positively impacted employees' cyber-security awareness within the firm. Some participants stated the cyber-attack had increased the firm's and its employee's cyber-security awareness. A few participants argued that this was because

individuals had seen what happened last time and were now more conscious and proactive in terms of security.

> FG1P1: *'in terms of personal awareness and how that affects you, as an employee but also company and, and everything, I think because we all had this experience, to kind of have the community thinking on the same attack, so it's not a hypothetical scenario, this is quite real.'*

In addition to the perceived increase in cyber-security awareness, some participants also discussed behavioural changes *'in the way people are going about their day-to-day jobs'* (G2P1), that they saw take place after the attack. For example, one participant, who worked for the cyber-security team, said they had seen an increase in the number of people who would check with them that a project was secure before going ahead with it, and another mentioned that they got more reports of phishing and scam emails from employees than before the attack.

Some participants mentioned that the attack had initially increased individuals' awareness of cyber security within the firm, but that because it happened a few years ago, this initial shock factor was beginning to lessen, and people were beginning to forget. A few participants mentioned that for some the attack was still in their minds but that others *'potentially have not kept that in mind and are probably at risk falling into the same habits potentially'* (G2P4). It was argued that individuals were on high alert immediately after the attack, but over time this alert mode reduced.

It should also be noted that the impact was not viewed as only affecting those employees present or working at the firm at the time of the attack. New joiners or those that had joined since seemed to also be knowledgeable of the attack and the perceived impact it had on the firm.

> FG6P12: *'I wasn't here before the cyber-attack so I don't know the difference between what yeah protocols were before and after but I know that he's definitely fundamental parts working at the firm yeah and I still heard about the attack.'*

FG5P10: *'Yeah… I worked for the company 10 years ago and then left but I recently Came back kind of about back about 17 months ago now. I did hear about it because I was still keeping you know in this or like the latest or like loop.'*

However, a few participants thought that maybe those who were not employed at the firm at the time would not *'understand quite as much'* (FG3P6) or that it would be *'a little bit more past history'* (G1P1). Meaning that those who had not experienced the attack first hand might be less aware of the impact of a cyber-attack. However, participants mentioned that these people were still made aware of the events occurrence, and that the attack was still spoken about. However, it was mentioned in the elite interviews that the cyber-attack was not used as a case study in cyber-security training or awareness materials.

Although the vast majority of participants saw the cyber-attack as having a lasting and positive impact on the firm, either because it reduced risk, created better security through policy changes and security measures, or increased the firm's awareness, a few participants stated that the attack did not have a lasting impact on employees in general as the repercussions of the attack had been dealt with in the background and employees did not have to think about this. Other participants argued that the attack had been forgotten about, and people were moving back to their old behaviours and habits that were perhaps less secure.

G2P4: *'But there are a number of individuals who study the idea* [cyber security] *within IT that seem to have completely forgotten how that all went down. So, the reintroduction of crappy software on the network, for example is you know, essentially restarting that cycle again, what could be the next cyber-attack.'*

A few participants stated that employees were able to just carry on as normal, as everything after the attack was just fixed in the background. For example, one participant stated that *'there might be systems not be working very different ways behind the scenes, but it's not something that we are sort of aware of'* (G2P8), which puts forward the view that systems

and security might have been changing, but this is not something the general employee was attuned to.

Overall, this subtheme demonstrates that the majority of participants understood the cyber attack at the firm to have had a significant impact on the organisation. This impact was generally viewed to be positive, leading to an increase in awareness and more secure systems. Participants also displayed 'it couldn't happen again' type of thinking. A few participants expressed the view that the effects were not perhaps as lasting as others thought and that although the systems might be being made more secure, the typical employee was not aware of this and did not have to behave differently.

5.4 Pessimistic Beliefs

Although optimistic beliefs were dominant in the findings, a smaller number of participants expressed more negative beliefs regarding the likelihood of being a victim of a cyber-attack, and more broadly related to the firm and their cyber security position. This data had fewer references than the data surrounding more optimistic beliefs. However, this still came out as a small theme in the data and demonstrates individual differences between employees at the firm. Ideas related to the firm's likelihood to fall victim to a cyber-attack were often due to the general nature of cyber-attacks and how prolific they were or because of law firms having access to sensitive information. A few participants mentioned that cyber-attacks were common, which increased the risk to the firm.

> FG1P1: *'Well, I think cyber-attacks are still on the top 10, you know risks, probably worldwide, so you know and yeah, we're still very likely to be a victims.'*

Whereas other participants referenced how they were frightened of specific scams that aimed to take money from the victims. One participant argued that cyber criminals might have a specific vendetta *'to probably try and you know get into you know, the business to do, you know serious harm'* (FG5P10).

FG5P11: *'I think of people trying to destroy the business and the kind of political situation and people trying to scam money from you saying 'click on this link because we've lost your details' or something like that. So yeah, those are the kinds of things from I'm particularly frightened of.'*

This can be seen as a contrast to the subtheme on the optimism bias and other positive self-serving biases, as here it was clear participants believed their firm specifically was at a lower risk, owing to a number of reasons, such as good security measures and good security awareness, often in comparison to other organisations. This view is evidence of individual differences between employees who have almost directly contrasting views.

However, it should also be pointed out that some participants expressed both beliefs. As evidenced above, FG1P1 expressed that they were likely to be a victim because cyber-attacks were considered a high risk both at the firm and personally. However, as evidenced below, they also stated that the firm would be less likely than others to fall victim to a cyber-attack because of reasons such as the previous cyber-attack and being well prepared. Hence, adding a positive spin to the perceived risk was the prevailing attitude. The quote below is from the same participant (FG1P1) who above stated that the possibility of a cyber-attack is a very high risk for organisations globally.

FG1P1: *'I suppose likely, it's very likely because we already lived through one cyber-attack, and because of the global reach, you know, some offices are in countries that are better at cyber attacking than others but because we've been through exercises, I think our vulnerability is quite low because we learnt a lesson quite severely'*

Other participants suggested that certain colleagues were more likely to fall victim to a cyber-attack or phishing scam or put the organisation at risk because of certain behaviours they displayed. For example, one participant mentioned that they previously worked somewhere where people kept passwords written down on their desks and stated they believed this type of behaviour to happen everywhere. Such participants would also display positive attitudes towards the organisation's overall risk. Again, this suggests that sometimes when participants thought negatively about cyber-security behaviour within the organisation, they would argue

that this also happened in other organisations or try and put a positive spin after stating something negative. This could suggest that employees were displaying optimistic views while ignoring conflicting evidence. This could also suggest that participants were unwilling to be wholly negative about their organisation due to a social desirability bias.

> FG5P11: *'I think I have heard of people and sending messages from other people's PCs where they've left it on so it's just been in a jokey kind of way, but I think it does provide security risks yeah'*

This discrepancy suggests that even when participants pose negative views or mention non-compliant behaviours, they add a positive view of the risk as a whole. Furthermore, optimistic and pessimistic beliefs can be seen as ways for participants to understand risk simply and are both biases that might happen in response to potential risk.

Overall, this smaller subtheme demonstrates that some of the participants put forward slightly more negative views relating to the general cyber-security risk of the organisation. However, as demonstrated above, these participants would often go on to then add a positive spin to this or give evidence as to why this might not be the case for their specific firm. This could suggest that although participants might have negative views, they were unwilling to be wholly negative about their organisation.

5.5 Perceived Threats: Human Factors Versus Others

This theme looks at the most common cyber-security threats perceived and mentioned by participants within the organisation. Therefore, this data assists an understanding of what participants viewed to be the threat landscape within the context of their organisation. This subtheme also sets the scene for later subthemes in this chapter, such as the view of the human as a hinderance to cyber security. As mentioned in the literature review, previous research on perceived threats to employees has often amalgamated employees from many different organisations. Thus taking away the meaningfulness of how context might influence

threat experience. For example, survey and questionnaire answers might be 'averaged' in order to gain general trends.

One of the biggest concerns in the data for the participants was the cyber-security risks involved when working with clients. Clients pay for the service they receive from law firms, and they expect information and data handling to be secure (Duc-Bragues, 2015). Working with clients also involves large amounts of data to be handled correctly and constantly being passed between two or more parties, as well as money handling. This is not something specific to the law sector, as many industries handle client data. However, law firms may be privy to extra sensitive data, especially as the current organisation is one of the world's leading business law firms (Lorsch & Chernak, 2006).

> G2P1: *'This is the way that business models work unfortunately, this is a law firm our business model is we take our clients data and then quite often email it to someone else. If we are doing a contract negotiation, we will take a lot of information from the client'*.

Participants described many examples within data handling and client processes. One participant described a situation they had been through where they got an email from what appeared to be their current client *'a link for documents to be opened and it was posing as a new instruction from the client'* (FG1P2) but was in fact not their client. However, they were able to contact the client to check before opening the link and documents and before complying with the new set of instructions.

> G2P7: *'we've seen WannaCry style ransomware infect client systems and payment being demanded.'*

Additionally, and still relevant to clients, participants mentioned that threat actors had contacted their clients before pretending to be from someone inside their firm.

> G2P6: *'so where people contact us pretending to be someone else or they've contacted our clients pretending to be us at the firm.'*

Another commonly mentioned threat was the broader threat of phishing, whereby outside actors attempt to phish employees within the firm. For example, cyber criminals may try to get employees to click on a link or send them money by masquerading as a trusted identity, such as another employee within the firm or a client. Participants gave examples of when phishing attacks had been attempted within the firm and in their personal lives. These were often very detailed, and the quotes below represent snippets of these examples.

> G1P1: *'there was the cliché Nigerian Prince that came through trying to ask us for kind of information, but at the same time there were other people who sent very odd strange things'*

> G2P6: *'There was another one where the fraudsters had pretended to be from… well they'd actually use the real the identity of a real person in our firms credit control team.'*

Participants also mentioned employee behaviours as potential threats. Some participants mentioned that employees would occasionally deliberately circumvent policies. For example, one participant argued that if lawyers need something done, they try to find *'ways around security'* (G1P3) procedures in order to speed up the process. Others mentioned that convenience played a factor in not complying with certain security policies.

> G2P5: *'I think it's convenience in the sense that if the laptop isn't working properly, if it's more convenient to use your own laptop, if you can get the job done quicker.'*

> G2P4: *'Like any organisation we face individual circumvention of controls because they* [employees] *don't know any better. Or they think that they have the authority to do that. I think the circumventing controls is a good one* [example] *because people don't always appreciate the risks that comes along...'*

However, other participants argued that employee-related risks were usually mistakes rather than deliberate actions. Participants mentioned that stress or a lack of attention could lead to

accidental mistakes that could cause potential harm. Moreover, by not fully applying their minds to tasks, they could fall victim to an attack that way.

> FG2P3: *'I think it's if you're multitasking and if you're particularly busy or stressed or whatever it is possible I think to click on something before you realise what exactly it is you're doing and then it's too late, so that that's almost my worry.'*

Participants also referenced physical security risks, such as people writing down passwords because they could not remember them and having their computer with them to work when travelling, for example, on trains.

Participants also spoke about personal threats that they had experienced or heard of in their personal lives. This was often spoken about in relation to social media or issues with finance and bank-related security. These were also human factor related and referred to individuals falling victim to scams or personal information being read on social media.

> FG6P12: *'I think of speaking of PayPal. I think on like text as well. Yeah, there are new scams coming out where they disguise their name without even sending a number…'*

> FG3P7: *'I don't do social media websites, so I don't do Facebook, or anything like that, which is a lot of time is it is open to attack and you've got lots of personal information on there…'*

Overall, this subtheme brings together data where participants spoke about threats to employees, the firm, and their personal lives, most of which were human factor related. It highlights that when considering possible threats, participants primarily spoke about client-related risks, phishing and human behaviours as their top concerns and did not highlight any technological factors. Client related risks were a large concern, as this also related heavily to data handling and the firm's reputation.

5.6 The Human as a Hinderance to Cyber Security

This theme brings together data of employee characterisations as to whether the human element is considered to be the underlying problem in cyber security. Cyber-security systems within organisations are made up of many interconnected components. However, generally within the data, cyber systems were seen by participants to be split between the technological and the human side. Broadly, it was clear from the data that most participants saw the human element to be the firm's main cyber-security problem. As both junior employees and those in more managerial senior positions were interviewed, this subtheme will first establish how lower-level employees believed they were viewed by management. Secondly, the subtheme will look at how senior employees viewed those they manage.

It was clear that the more non-managerial set of employees believed that humans were viewed as the main limitation to an organisation's cyber security.

> G1P3: *'I would think that humans are still pretty much the vulnerability when it comes to information security'*

> G1P1: *'I just think they* [managers and the information security team] *will look at I guess us as the weak link. We are the unknown.'*

Participants here generally referred to others, rather than directly referring to themselves as the vulnerability. Participants also cited possible behaviours or attitudes they saw in employees in the firm that they believed might heighten the firm's vulnerability. For example, one participant argued that, when it comes to cyber security instances, it is *'generally it's someone clicking on a link or opening an email'* (G1P7).

> G1P3: *'I mean, I would think that humans are still pretty much the vulnerability when it comes to information security. Yeah. In my department I don't think I get much social engineering or anything like that but more carelessness and not necessarily ignorance, but just being unaware of what best practice is or what they should be doing or the implications of not following practice.'*

Not only do these quotes demonstrate that the participants believe they were viewed as a vulnerability, but participants also believed this to be true themselves. This is evidenced by participants arguing that 'they view us' as the problem and 'we are the unknown'. Participants in this way seemed to accept that they were part of this unknown element of cyber security, rather than it being something they apply to others within the firm and not themselves.

This view of the human factor was often in contrast to views of technology or systems in place to protect against cyber-security issues.

> G1P7: *'Generally it's a people failure rather than a system failure, that you know, that could cause I don't know a virus or impersonation or I don't know hacking of emails. I mean, I don't know the terminology very well, but I do think often it's you know, an error from an individual that can cause that rather than the systems we have in place.'*

Technology, or 'systems' in this case, was viewed to be the more stable, more reliable entity, where it was less likely for cyber-security issues to occur. Another participant also argued that cyber-security incidents were often caused by *'leaving laptops on trains or losing mobile phone etc.'* (G1P9). A few participants noted that they did not think such behaviours had malicious intent but were simply human mistakes.

Similarly, the majority of more senior participants interviewed also believed the human factor to be the main prolific vulnerability in cyber security.

> G2P1: *'…at the end of the day security is a human problem, security is a people problem fundamentally, human nature kicks in, and people will try to, if you put controls in place, people will try to bypass them not because of malicious intent just because human nature kicks in…'*

As evidenced by the above quote, some employees did not believe the human factor problem to be of a malicious nature but had formed an understanding that it was habitual for

humans to make errors or that it was human nature to try and circumvent policies. Other participants stated that employees might break policy protocol in order for them to do their jobs more efficiently and, in this way, presented a semi-understanding view of why humans might be a vulnerability.

> G2P10: *'you can put all the technology in place but if it's not straightforward for people to do their jobs, they're gonna try and circumvent it or find ways around it…'*

> G2P4: *'computers don't do bad things people do bad things'*

This quote further demonstrates the perceived split between technology and the human element. Participants argued that they would be more concerned about *'a member of staff performing some sort of security breach than of a technological you know, an outsider the managing to break into our systems'* (G2P3), demonstrating that the main worry was with employees inside the firm, rather than someone breaking through their technological safeguards from the outside.

> FG5P10: *'Yes, the policies are pretty and utterly watertight, so I'm if I'm honest… I think it's down to individuals like following them.'*

This is also supported by the idea that, when talking about cyber-security risks more generally and indirectly, participants referenced human behaviours as something that increased risk and the technological security layers as something that reduced risk, even if they were not directly compared. For example, some participants stated that employee vulnerability to phishing emails was a big risk for the firm. Other participants mentioned password behaviours and employees circumventing policies as actions that might increase the firm's cyber-security risk.

> FG1P4: *'yeah it would be it would be lack of attention it would be lack of due care and attention I think would be the biggest risk for me would be.'*

> FG4P9: '*I feel like doing stuff like connecting like to the VPN is like one way that like I keep like information secure.'*

This contrast is demonstrated above, where one participant talks about 'not paying attention' being the biggest risk for them, in contrast to another employee referencing the VPN as a way in which they are able to keep information secure.

Lastly, within this narrative, it was also clear from the data that many participants blamed the cyber-attack on human error within the firm, even though the firm was hit via a supplier. This again suggests a narrative where employees are willing to blame the human element, in this case, employees within the firm, rather than the actual chain of events. However, it is possible that they do not have knowledge of the chain of events and that the narrative stated is the narrative told to them by other employees within the firm.

However, there were a few junior employees (2 participants) and managers (4 participants) that did express some view that humans were an important asset to cyber security or expressed the view that seeing the human as the prevailing vulnerability in cyber security is more a thing of the past.

> G2P10: *'I actually kind of flipped that phrase on its head now and where, yes people used to be seen as the weakest link, we now see it as people can be, talk about the human firewall, and say that people can actually be our strongest asset.'*

In the quotes above, the term 'weakest link' was likely used by the participant because they were asked whether they believe the human to be an asset or a weak link to cyber security. However, in a few other interviews, the terms 'weak link' or 'weakest link' were used unprompted by the researcher. Given the specificity of this phrase, this might suggest that these participants have seen or heard use of the term 'weak link' in reference to the human in cyber security, which could further contribute and add to this viewpoint. Other participants used terms such as 'the issue' or 'vulnerability' when asked directly how they themselves and the human was viewed.

A few participants also mentioned that it is important to educate and train employees for them to be part of the solution, for example, saying they could be security champions for the organisation. Another participant also mentioned that new employees joining the organisation are *'so tech savvy'* (G2P1), and in this way saw them as important in the development of security in terms of technology. This suggests that some participants did see the benefit of the human factor.

EI1 and EI2 stated that the organisation wanted to be more 'human-factor focussed'. The view of employees as a solution to cyber security rather than a hindrance to cyber security was put forward by EI1 in the original conversations that took place when arranging the logistics of the case-study research project with the organisation. In both elite interviews, the participants described how they wanted to inspire employees in the organisation to take responsibility for their own actions and make a positive impact on cyber security.

> EI1: *'…I really do want to empower people to a take responsibility for their actions and of make them heroes for the business, if they spot an attack and let us know before anyone's clicked it, that's really, really crucial'*

> EI2: *'we've created a human element, I don't think that's the right word… but we have created you know, an approachable element over the last 18 months'*

One of the elite interview participants mentioned that this aim to be more human-centric and human factor positive, although largely led by their team, also resonated with higher management.

> EI1: *'So I think my bosses, the CISO and my direct line manager we're hearing a lot more about human so they both come from technical backgrounds, very technical backgrounds, but they were hearing more and more in the industry about the human factor yeah and how it shouldn't be the kind of weakest link and so that's why they hired me.'*

This suggests that even the more technical roles within the cyber-security department were interested in the human side.

In summary, this subtheme 'the human as a hinderance to cyber security' demonstrates that junior employee participants and participants with a managerial role view the human as the 'problem' in cyber security. This is seen in contrast to the technological and systems side of cyber security, which is seen to be stronger and more reliable. However, a few participants in the firm did put forward ideas surrounding the employee as an asset to cyber security and suggested that the human as the weak link was a view of the past.

5.7 Summary

This findings chapter encompassed subthemes surrounding the umbrella theme of the individual human element. These subthemes demonstrated that many participants expressed optimistic and self-serving views of cyber-security risk, especially related to the organisation. A few participants communicated their understanding of a dichotomy between their personal lives and their role within the firm. However, some individuals did additionally display some more pessimistic ways of thinking. The optimistic views were also related to participants' understanding of the firm's cyber-attack in 2017. Participants argued that the attack had a wide impact on the firm, increasing awareness and perhaps ensuring that another similar event would not happen to the firm again. Finally, the data showed that most participants viewed themselves and other employees (what we refer to as the human element) as the main 'problem' in cyber security and believed others viewed them as such. This was due to referenced behaviours and comparisons to technology.

5.8 Discussion

This discussion section synthesises and grounds the findings from this chapter within the research and theory from the literature review. This chapter encompassed subthemes that emerged from the data as internal perceptions and biases and how employees viewed and

are viewed in the context of cyber security. The findings suggest how many participants offered views that were seemingly optimistic and how this related to views of a cyber-attack experienced by the firm in 2017. In this section, such findings will be related to previous studies of the optimism bias in the context of cyber security (Campbell et al., 2007; Chmielarz & Szumski, 2019; Cho et al., 2010; Haltinner et al., 2015; Kim et al., 2018), as well as how such thinking strategies are conceptualised by psychological behaviour change theories (Prentice-Dunn & Rogers, 1986; Witte, 1996). The discussion will further look at the concept of fatalism in contrast to optimism and how such cognitions fit within the wider literature and theory (Lawson et al., 2016; Penney, 2019; Xie et al., 2019). The repercussions of the 2017 cyber-attack, as perceived by the participants, will be compared to previous research looking at the impact of cyber-attacks (Bada & Nurse, 2019; Knight & Nurse, 2020; Stacey, Taylor, Olowosule & Spanaki, 2021). Finally, this section will look at the participants' negative views of the human factor in the context of the usable security and positive security dialogue and research (Parkin et al., 2010; Reinfelder et al., 2019; Sasse et al., 2001; Zimmermann & Renaud, 2019) as well as how such views could influence participants' self-efficacy or control beliefs in the context of PMT (Prentice-Dunn & Rogers, 1986), the EPPM (Witte, 1996) and TPB (Ajzen, 1985).

5.8.1 Biases

The optimism bias or unrealistic optimism refers to a perception of one's personal vulnerability; a tendency of individuals to generally believe that adverse events are more likely to happen to others than to themselves or to overestimate the likelihood of experiencing positive events and underestimate the likelihood of experiencing negative ones (Weinstein, 1980). This optimism was a view consistently demonstrated by participants within the current study. This result is, therefore, comparable to other pieces of research that have demonstrated the presence of an optimistic bias in risk perceptions associated with cyber security (Campbell et al., 2007; Chmielarz & Szumski, 2019; Cho et al., 2010; Haltinner et al., 2015; Kim et al., 2018; Rhee et al., 2005; Rhee et al., 2012). The current findings add to the current literature on the optimism bias in cyber security in a number of ways. Firstly, the results demonstrate that participants believed their firm to be better than others in terms of

cyber security, which would mean negative events would be less likely to happen to them and the firm. This shows a collective form of optimism that extends to the whole organisation, which is an important finding as previously optimism bias research in cyber security has been relatively individual (Campbell et al., 2007; Chmielarz & Szumski, 2019; Cho et al., 2010; Haltinner et al., 2015; Kim et al., 2018; Rhee et al., 2005; Rhee et al., 2012). Therefore, the current research contributes to our understanding of cyber-security biases by both corroborating and extending previous research on the optimism bias in cyber security. Secondly, most previous research has not been conducted within an organisational context outside of universities (Campbell et al., 2007; Chmielarz & Szumski, 2019; Cho et al., 2010; Haltinner et al., 2015; Kim et al., 2018; Rhee et al., 2005) or has looked only at information security experts (Rhee et al., 2012). Finally, most of this previous research has been survey or questionnaire-based (Campbell et al., 2007; Chmielarz & Szumski, 2019; Cho et al., 2010; Kim et al., 2018; Rhee et al., 2005; Rhee et al., 2012) with qualitative interview-based research only found in student populations (Haltinner et al., 2015). Therefore, the current research extends previous research on the optimism bias within cyber security by expanding findings to include the optimism bias in terms of a belief that one's organisation is better than others. Moreover, the current findings demonstrate the bias within an organisational context and deepen previous examples of this finding by using a qualitative case study. This contributes to research by demonstrating the extent of the bias. This is important as biases impact cyber-security behaviour.

When thinking of cyber-security threats, participants in the current study generally referenced those pertaining to human factors. This fits in with previous research demonstrating that individuals often focus on human-related risks when they think of or rate cyber-security risks. For example, Van Schaik et al. (2017) found that participants in their study were most frequently worried about identity theft, which they believed to be owing to perceived personal consequences as well as press coverage, which may have increased the ease of availability of relevant examples. Previous research in cyber security has demonstrated that many factors influence peoples' risk perception of security threats and that individuals' risk perceptions of cyber-security threats often differ from actual risk (Nurse et al., 2011b). The focus on human factors as threats could be due to participants' personal experience or information they receive and the environment in which they receive this

information. Firstly, we will look at their personal experience and how this may influence threat perceptions. As we have seen in the previous chapter, many participants believed the cyber-attack experienced by the firm was due to human risk, both internal and external to the firm. This may predispose individuals within the firm to believe the human risk to be the highest kind of risk, even if, as previously demonstrated, they do not believe the firm to be particularly at risk of falling victim to cyber-security threats. Previous research demonstrates that previous experience in and awareness of cyber-security threats increases the perceived threat (Nam, 2019). Therefore, the current research offers support for these findings. Moreover, as demonstrated within the literature review and previous findings chapters, both industry, research, and popular news outlets have very much focussed on the human factor as the main risk to cyber security. Researchers have demonstrated this to be a possible harmful dialogue for people, owing to reduced efficacy (Beautement et al., 2008; D'Arcy et al., 2014; Inglesant & Sasse, 2010; Renaud, 2011). Within industry, this dialogue is likely also because most employees cannot do anything about certain technological risks, as this remains a function of the cyber-security team. Therefore, employees are encouraged to focus on risks and behaviours they can impact. Research demonstrates that risk perceptions play a fundamental role in models as predictors of precautionary behaviour (Haung et at., 2011).

The fact that the main risks highlighted by the participants were human factor related could therefore be an example of the availability heuristic. Tversky and Kahenman (1974) identified three main types of heuristics that they believed individuals employ when making judgements under uncertainty, and that can give way to biases and errors in decisions. The availability heuristic is where people judge the likelihood of an event happening based on how easily they bring an example to mind (Harvey, 2007). For example, if one is thinking of flying and then suddenly remembers a few recent airline accidents, one might feel like air travel is too dangerous and decide to travel by car instead, even though car travel is statistically more dangerous (Van Middelkoop et al., 2003). Human factors in cyber-security feature prominently in industry publications, government-sponsored events and publications (Goo et al., 2014; Hughes-Lartey et al., 2021; Lowry & Moody, 2015; Sabillon, 2022). Moreover, as discussed, the firm experienced a cyber-attack, believed by many to be human factors related. Therefore, the current research supports previous literature where the

availability heuristic in cyber security has been proposed and argued to impact perceptions (McAlaney & Benson, 2020; Tsohou et al., 2015) and research (Ashenden, 2018) in this domain. At the time of writing, to the author's knowledge, the availability heuristic has not yet been empirically studied in relation to cyber security. Therefore, the finding is important, as it demonstrates another possibility of a perceptual bias with regard to cyber security, which may help future policymakers better understand the mindsets of individuals.

Participants in the current study also displayed pessimistic and fatalistic beliefs. Fatalism refers to an outlook where risks are controlled by external forces along with a view that the participants as individuals are powerless to change this, or where individuals passively deny personal control of a situation to an attitude of resignation in the face of events that are thought to be inevitable (Niederdeppe & Levy, 2007; Xie et al., 2019). Previous research related to cyber security has found evidence of fatalism in the context of privacy (Xie et al., 2019; Penney, 2019) and fear appeals (Lawson et al., 2016). The current research extends these findings by showing the presence of possible pessimistic beliefs within an organisation. Such findings are important as research into the effects of fatalistic beliefs on health behaviours illustrates that those who hold fatalistic beliefs are less likely to engage in preventative behaviours and measures (Jonnalagadda et al., 2012; Niederdeppe & Levy, 2007). Moreover, those who hold fatalistic beliefs about a particular health risk may be more likely to develop the said health risk because they are less likely to engage in prevention behaviours (Niederdeppe & Levy, 2007). However, as previously noted, these were not the prevailing views, and participants often displayed such beliefs in addition to optimistic beliefs. Moreover, participants in the study did not overtly display feelings of being powerless to change the situation, meaning that beliefs were perhaps more pessimistic than they were fatalistic. Additionally, although participants expressed beliefs that can be considered pessimistic, it could also be argued that such beliefs were realistic, given the real threat of cyber security risks to firms (National Cyber Security Centre, 2021).

More broadly, the findings of the optimism bias, and other perceptual biases, fit with the wider psychological literature on the ability, or lack thereof, of individuals to perceive threats ‘accurately’ (Lichtenstein et al., 1978). Risk itself is subjective, with many researchers referring to it as socially constructed and psychologically orientated, meaning that perceived

risk and actual risk can often be quite different (Slovic, 1987; Slovic et al., 1980). People's understanding of cyber-security risks has been shown by research to mimic Slovic's (1987) earlier work, demonstrating that many factors influence people's risk perception of security threats and that people's risk perceptions of cyber-security threats often differ from actual risk (Nurse et al., 2011b). Again, the current findings add to existing research on perceptions of risk within cyber security by demonstrating the presence of the optimism bias within an organisational context and deepening previous work with case-study based qualitative research.

Discussions of the cyber-attack experienced by the organisation in 2017 were also a large subtheme that emerged from the data, which further presented the possibility of biases. The cyber-attack was viewed to have a significant impact on the firm. Broadly speaking, this finding fits in with much previous scholarship looking at the impact of cyber-attacks, which has found cyber-attacks to significantly impact nation-states, governments, economies, people, organisations and their employees, and security infrastructure (Bada & Nurse, 2020; Czosseck et al., 2011; Genge et al., 2015; Gupta & Agarwal, 2017; Knight & Nurse, 2020; Stacey et al., 2021). Research has shown that cyber-attacks do not only impact policy and technology but may also have a psychological and social impact on people and societies who experience them (Bada & Nurse, 2020). Moreover, the specific cyber-attack experienced by the firm, NotPetya, was devastating for many organisations as businesses across industries were affected without having an opportunity for system recovery (Lika et al., 2018). Some have even argued that NotPetya was one of the most devastating cyber-attacks in history for organisations (Greenberg, 2018). However, the attack was generally framed in an optimistic light within the current organisation. Participants argued that the cyber-attack had a lasting positive for the firm in many ways. Participants displayed beliefs that the firm was now more secure, they were ahead of the game, the attack increased employee cyber-security awareness and that it was a one-time occurrence, and they were now less likely to be the victim of another attack. This, without further analysis, would extend previous research by demonstrating that people can often perceive positive outcomes from cyber-attacks, such as improved awareness, that they believe will help the firm in the future. Previously, research has primarily highlighted the negative impacts of a cyber-attack (Bada & Nurse, 2020; Czosseck et al., 2011; Genge et al., 2015; Gupta & Agarwal, 2017; Knight & Nurse, 2020). The

current research corroborates findings from Stacey et al. (2021), who found that post cyber-security attacks, participants understood the seriousness of such cyber-security policies and adhered to them better. Moreover, the current research provides evidence of impact on a more longitudinal basis. It should be noted that the current research took place three years after the cyber-security attack. Therefore, it is possible that negative experiences and examples of impact may have been more prominent closer to the event.

However, despite the corroborating evidence that a cyber-attack may lead to a positive change in employee views towards cyber security, the belief held by participants in the current study that another similar event was unlikely to happen again could be seen as a form of the optimism bias. Researchers and industry professionals who have studied NotPetya agree that it could happen again or even reoccur on a larger scale (Greenberg, 2018). Moreover, research shows that up to 50% of organisations experience recurring cyber-security attacks, often from the same attackers (Ponemon Institute LLC, 2021). Not to mention the constant threat a range of cyber-attacks are said to pose, with multitudes of cyber-attacks being reported weekly (National Cyber Security Centre, 2021). This suggests that participants in the current study were optimistic in believing that a cyber-attack would not hit the firm again. This finding then, in turn, may further support the previously discussed evidence of the existence of the optimism bias in relation to cyber security (Campbell et al., 2007; Chmielarz & Szumski, 2019; Cho et al., 2010; Haltinner et al., 2015; Kim et al., 2018; Rhee et al., 2005; Rhee et al., 2012). This finding lends further insights to these previous studies by demonstrating that participants were optimistic about the firm's risk of a cyber-attack, even when a cyber-attack had previously impacted the firm. This suggests that even experience of an adverse event may not lead to perceptual changes in risk. It could be argued that not all participants would have been at the organisation during the breach and therefore did not experience it first-hand. However, participants argued during interviews that even those who were not present at the firm at the time heard stories about it and that the attack was part of the firm's culture and narrative, ensuring that employees were well aware of the attack.

5.8.2 Usable Security

In the current study, both security professionals and non-security professionals displayed consistent views that humans are the main vulnerability in cyber security and that participants believed that they were part of the issue. This fits in with a prevailing narrative within cyber-security research and industry that the human continues to be the main vulnerability in security systems (Goo et al., 2014; Hughes-Lartey et al., 2021; Lowry & Moody, 2015; Sabillon, 2022), making the objective of security professionals and researchers to eliminate the human component. This view remains despite research demonstrating or arguing for the contrary (Beautement et al., 2008; D'Arcy et al., 2014; Inglesant & Sasse, 2010; Renaud, 2011), or at least research arguing that this view is not only unhelpful but an impossible goal considering the extent of human-computer interaction within organisations. Additionally, research has shown that this belief, along with a lack of communication and understanding between security professionals and employees, leads to poor communication methods, cyber-security awareness strategies and cyber-security training (Inglesant & Sasse, 2010; Kirlappos et al., 2013; Renaud, 2011; Sasse et al., 2001; Sasse & Rashid, 2021).

Research has further argued that this belief blames the user while not considering policy faults and the sophistication of attackers. However, in a study investigating insider threats, Posey et al. (2011) demonstrated that employees who did not feel that their organisations trusted them would engage in more computer abuse when new security measures were introduced. This highlights that blaming the user may have unintended negative consequences. The attitude may also lead to the development of cyber-security behaviour metrics that do not consider many human factors. For example, phishing campaigns may give an easy metric of 'who clicks' on a link, but they do not give insight into why individuals may click or how best to help individuals stop doing so (Kirlappos & Sasse, 2011; Kumaraguru et al., 2009; Kumaraguru et al., 2007; Sheng et al., 2010). Therefore, the negative connotations of the users as the weakest link have led researchers to argue that the continued use of this narrative is restraining development in the field (Mc Mahon., 2020).

The current research adds nuance to existing findings of the human as a weakness dialogue. Previous research has largely highlighted that security professionals, IT workers and business

professionals see the human as the weakest link and that employees put organisations at risk (Goo et al., 2014; Hughes-Lartey et al., 2021; Lowry & Moody, 2015; Sabillon, 2022). This idea features prominently in industry publications and government-sponsored events and publications. Moreover, researchers themselves have added to this narrative by describing the human as the weakest link throughout their research (Goo et al., 2014; Hughes-Lartey et al., 2021; Lowry & Moody, 2015; Sabillon, 2022). However, the current research further demonstrates that within an organisational context, employees also think of humans as the weakest link and understand themselves to be seen this way by security professionals and managers within the organisation. This adds to the current research by demonstrating that not only are employees viewed this way by security professionals, but the employees know they are thought of like this. This view prevailed in the participants despite the elite interviews, stating they were attempting to change this dialogue in order for the human to be part of the solution. As the current research has demonstrated, through the many themes that emerged from the data relating to culture, individuals and policies, employees and their actions do not exist in a vacuum. Employee perceptions and subsequent behaviours regarding cyber-security risk are shaped by a vast array of beliefs, social relations, and workplace interactions and practices. It is, therefore, possible that employees believe this about themselves because of the dialogue put on them through the belief of IT and security professionals, both inside and outside of the organisation, as demonstrated by an array of research (Goo et al., 2014; Hughes-Lartey et al., 2021; Lowry & Moody, 2015; Sabillon, 2022). This, along with the research showing the problems this view propagates, questions who is being served by this dialogue and how we can expect employees to act if they are described as the weakest link.

5.8.3 Psychological Theory

In light of findings presented in this chapter, PMT and PMT related constructs may explain why participants demonstrated optimistic beliefs about the likelihood for the organisation to fall victim to an attack, as well as beliefs that an attack would not happen again, whilst also describing the human element as extremely vulnerable within the cyber-security sphere. Firstly, it could be argued that the cyber-attack increased threat severity. Threat severity is

the perceived degree of harm associated with an organisation's cyber-security threats, should they occur. In the case-study organisation, the cyber-attack caused a high degree of devastation to the firm (Financial Times, 2017; Lika et al., 2018), meaning concepts of threat severity were likely present in most participants. It can also be argued that the cyber-attack increased threat vulnerability, the degree to which participants believe an organisation is susceptible to an attack. Although, this point could be argued against given that participants primarily stated they thought the organisation was less vulnerable post the attack. When individuals assess threat vulnerability and threat severity, fear is often generated (Prentice-Dunn & Rogers, 1986). In order to reduce fear, the threat appraisals need to be matched with high response-efficacy and self-efficacy (the coping appraisal) in order for people to then engage in protection behaviours and adaptive engagement as part of protection motivation (Prentice-Dunn & Rogers, 1986). If employees do not feel they have enough efficacy to deal with the threats, coupled with a high threat appraisal, they might engage in maladaptive coping mechanisms. Believing oneself and the human element to be the weakest link in cyber security could be construed as a clear indicator that employees had a low coping appraisal, decreased self-efficacy, and decreased response-efficacy (Prentice-Dunn & Rogers, 1986). Not only did employees in the current study believe the human element to be the weakest link, but some participants also mentioned that this would 'always' be the case. Therefore, in the current study, it could be argued that employees had a high threat appraisal and a low coping appraisal. Therefore, it is possible that the optimism bias concerning the organisation's threat and the likelihood of a cyber-attack to happen again was a maladaptive coping mechanism in response to the high threat appraisal (Scheier & Carver, 1985). Therefore, the optimism bias about the cyber-attack could be a response to a feeling of not being able to protect oneself. However, previously maladaptive coping responses have primarily been shown to be fatalistic in nature (Kraus et al., 2015).

In addition, findings of the availability heuristic can be further deepened by using the lens of PMT (Prentice-Dunn & Rogers, 1986) and the EPPM (Witte, 1996). Both of these theories ultimately propose that in order for people to take precautionary action, individuals must have an increased sense of self and response efficacy and a perception of threat. If one's perception of a particular threat is higher than the combination of self and response efficacy and individual feelings towards a threat, they may be disinclined to take action or react with

maladaptive behaviours (Prentice-Dunn & Rogers, 1986; Witte, 1996). In the current research, participants named human-related risks when describing threats in cyber security. However, participants also perceive themselves and humans in general as the weakest link, suggesting low efficacy. Therefore, under the lens of PMT and the EPPM, participants in the current study may not be correctly motivated to behave securely. This would support previous research, which has found that high amounts of fear combined with high efficacy led to the most significant amount of behaviour change, whilst high fear with low-efficacy messages produce defensive responses (Floyd et al., 2000; Witte & Allen, 2000; Peters et al., 2013; Tannenbaum et al., 2015).

Similarly to the process just described within PMT (Prentice-Dunn & Rogers, 1986), under the EPPM (Witte, 1996), the optimism bias could also be seen as defensive motivation within the fear control process. Here, suppose perceptions of the threat begin to exceed the perceptions of efficacy, which again could be argued to be the case given the previous cyber-attack. In that case, people will shift to fear control processes, where, instead of thinking about the threat and engaging in danger control processes, people will act to control their own levels of fear (Witte, 1996). The current findings would also then support previous research demonstrating the usefulness of the EPPM in understanding employee perceptions and behaviours, as well as arguing for the existence of these constructs (Chen et al., 2021; Zhang & Borden, 2020). For example, the current research is similar to that of Masuch et al. (2021), who demonstrated that participants who felt that they had little protection against ransomware were more fearful and therefore dealt with the topic more defensively, often by avoiding the threat.

On the other hand, it has also been argued by researchers (Chen, Turel & Yuan, 2021) that the optimism bias can play a direct and moderating role in reducing perceived threats. The researchers argue for an extension of PMT that includes reference to the optimism bias, at least in the context of e-waste. These researchers found that the optimism bias negatively influenced threat perceptions related to unauthorised information retrieval from the discarded e-waste, as well as also negatively moderating the relationship between perceived threat and protection intention (Chen et al., 2021). The authors here argued that the results of this study demonstrated that optimism bias plays a dual role in cyber-security risk

assessments. First, the optimism bias reduces risk perceptions. Secondly, the optimism bias may lead to under-weighing of the assessed threats when developing intentions to cope with them (Chen et al., 2021). This idea might explain the optimistic attitudes towards risk displayed by the participants in the current study, as the optimism bias would interfere with appraisals of threat. As far as the researchers can tell, at this time, this is the only study demonstrating and arguing for the optimism bias as an interfering factor within cyber security. However, other pieces of research have demonstrated that rational cyber-security actions and beliefs can be interrupted by different biases (Bulgurcu et al., 2010; Rhee et al., 2012).

The current research, therefore, may also lend support to this study and the extension of PMT argued by the researchers (Chen et al., 2021), as it demonstrates that the optimism bias overlaps and interferes with perceptions of cyber-security risk. Therefore, the current research lends support to the argument that the constructs of PMT overlap with the optimism bias in some form, even if as a maladaptive coping mechanism (Scheier & Carver, 1985), at least in relation to cyber-security threat perceptions and behaviours. However, given the qualitative nature of the data within the current study, it is not clear whether the optimism is a response to low protection motivation or whether the optimism bias interferes with threat appraisals (Chen et al., 2021). Future research should aim to investigate this further and tease out the nuances of the relationship between the optimism bias influences and threat appraisals.

To the researcher's knowledge, the TPB (Ajzen, 1985) has little, if any, previous research relating the theory to the optimism bias, perceptions of cyber-attacks or beliefs surrounding the human factor as the weakest link within cyber security. Therefore, it will not be used within this findings chapter to deepen understanding of the optimism bias from the themes. However, the concepts of control beliefs and perceived behavioural control might be relevant here. Control beliefs are defined as beliefs about the existence of possible factors that may enable or impede one’s ability to perform the behaviour and the perceived influence of these factors. Control beliefs lead to perceived behavioural control, which is defined as an individual's perceived ease or struggle in performing the behaviour (Ajzen, 1985). Control beliefs can be understood as similar to the PMT and EPPM concept of self and

response efficacy (Prentice-Dunn & Rogers, 1986). Therefore, in the current case, if participants did not have high behavioural control, owing to the belief that they, as humans, are the weakest link, this might decrease motivation in performing recommended cyber-security behaviours. This discussion extends previous examinations of the TPB in relation to cyber security by offering support for its concepts within qualitative data in the context of an organisation (Bulgurcu et al., 2010; Ifinedo, 2012; Kim & Mou, 2020; Sommestad et al., 2015).

5.8.4 Conclusions and Contributions

In summary, the discussion of the current findings pertaining to the individual human element concerning usable security scholarship and psychological theories highlights where this research has supported, added to, and been in conflict with previous work or demonstrated concepts of models within an organisational environment. Firstly, findings relating to the optimism bias demonstrated the existence of a collective form of optimism that extends to the whole organisation, which is an important finding as previously optimism bias research in cyber security has been relatively individual (Campbell et al., 2007; Chmielarz & Szumski, 2019; Cho et al., 2010; Haltinner et al., 2015; Kim et al., 2018; Rhee et al., 2005; Rhee et al., 2012). Secondly, this research contributes to existing dialogues by suggesting the possibility of the existence of an availability heuristic in relation to cyber-security perceptions. Moreover, similarly to existing work, the current research demonstrated that a cyber-attack which hit the firm in 2017 had a lasting impact on the firm (Bada & Nurse, 2020; Czosseck et al., 2011; Genge et al., 2015; Gupta & Agarwal, 2017; Knight & Nurse, 2020; Stacey et al., 2021). Although, the current findings extend previous research by showing that the long-term repercussions of the attack were often viewed positively. Reasons why this could be considered to relate to the optimism bias, were also discussed. The current research adds to existing findings of the human as a weakness dialogue as consistent views that the human was the main point of weakness for cyber security and that employees believed themselves to be the weak link. Therefore, the extent to which participants could have efficacy if they believed themselves to be the weak link was questioned. Finally, the results were discussed through the lens of psychological theory; PMT (Prentice-Dunn & Rogers, 1986), the EPPM

(Witte, 1996) and TPB (Ajzen, 1985). It was shown that the optimism bias could be both considered a maladaptive response to PMT constructs mechanism (Scheier & Carver, 1985) as well as a direct influence on individual threat appraisals (Chen et al., 2021). Thus, lending support to both ideas. Future research should aim to tease out these differences, perhaps in more controlled experiment-based studies. The TPB also offers insights in relation to the concept of control beliefs and perceived behavioural control.

Chapter 6. Perceptions of Cyber-Security Training and Policies

6.1 Introduction

Cyber-security policies and awareness training programmes are a long-term corporate investment for firms that aim to achieve better regulatory compliance, cyber-security behaviours, and culture. However, there are high levels of ambiguity on 'what works' within organisations. Unlike the previous chapters, which have generally focussed on individual and social perceptions of and nuances in cyber security, this chapter brings together findings where participants gave their views on the relevance of cyber security to their job role and cyber security organisational policies and training. By doing this, the chapter aims to look at 'what works' in terms of organisational policy and training from the participants' point of view as a reflection of broader employee perspectives. The data here also presents threat perceptions of participants in order to give context to what participants believed to be the most significant threats and how they subsequently viewed policy and their own behaviour.

As mentioned in the literature review, much previous research has looked at the effectiveness of specific cyber-security policies or training methods. Usually, effectiveness is measured by calculating cyber-security compliance or culture before and after the policy or training is implemented. However, such measurements are often arbitrary and do not consider the perceptions of participants or the context and setting in which such behaviours and culture develop and take place (Bada et al., 2019). For example, phishing methods have been questioned for poor metrics and ethics (Kumaraguru et al., 2009; Kumaraguru et al., 2007; Sheng et al., 2010). At the time of writing, no such research has been done in a case-study methodology within a single private organisation and hence does not take into account how individual organisations shape cyber-security behaviour and culture. This is significant as current training methods and policies are based on amalgamated research that may not recognise the nuances of cyber-security perceptions and behaviour. This then creates further issues for employees when training is put into place that does not have supporting contextual research. Therefore, the current research presents a realistic view of training and policy function within an organisation as perceived by participants.

The data within this chapter is separated into four subthemes. Firstly, the chapter will look at how participants understood their job role in relation to cyber security, specifically whether participants saw their day-to-day work as pertaining to cyber security. Secondly, the data surrounding cyber-security behavioural practices will be discussed. Then, the specific pain points those participants described will also be highlighted. Lastly, this chapter highlights the variety of opinions on the organisation's cyber-security training and awareness received by employees. After presenting these subthemes, the chapter will then discuss the findings related to the literature and psychological theory summarised within the literature review. The findings will use the usable security scholarship to put pain points into conversation with cyber security and psychological theory.

6.2 Perceptions of Job Role

This subtheme highlights data where participants deliberated whether cyber security was part of their job role or day-to-day at work. Day-to-day roles and business operations here refer to daily activities and behaviours that a firm and its employees engage in. This is an important data set to highlight, as generally, within the literature and wider cyber security discussions within industry, cyber security is seen to be, or at least those creating policy and training believe it should be, everybody's responsibility within organisations. Some organisations and literature even warn of the dangers of irresponsible and uninformed employees (Etsebeth, 2006; Hassanzadeh et al., 2020).

This subtheme has clear demographic differences. Those with IT and information security-related job roles saw cyber security as more closely involved in their everyday job than those who did not work in IT or security-related roles.

This subtheme, therefore, highlights the degree to which employees within an organisation see cyber security as relevant to their job role. The decision was made to put the perceptions of job roles within this theme, as often, the nature of a job role is partially decided by the organisation and the organisation's policies. However, the authors do note that this

subtheme relates to other findings on responsibility. Therefore, this particular subtheme epitomises the notion that the themes in these findings are all interconnected in some way.

Firstly, it is clear from the data that around half of the participants (out of those who spoke about cyber security in reference to their job role in the focus groups or interviews, as sometimes this topic was not covered) believed cyber security to be a large part of this. However, out of the 10 participants involved in focus groups or interviews who were in an IT or Information security role, 8 of them were within this half (out of 18 participants who stated they believed cyber security to be part of their job in total). Therefore, the majority of those with an IT role believed cyber security to be relevant to their day-to-day job role. This suggests that job role does have an impact on whether participants perceive cyber security to be part of their job when the job role is IT related. Although this finding it is perhaps not surprising.

> FG5P10: *'I work within the IT department and within local support so security can be a big thing in number sort of levels'*

The remaining 'non-IT / infosec' participants who saw cyber security to be part of their job role generally described this to be owing either to close relations with the cyber security team, because they worked on cyber security relevant projects, or because of client data and confidentiality policies.

> G2P7: *'I'm an associate lawyer in the litigation and regulatory team in Manchester, but my subspeciality or my main specialty is contentious data protection and cyber security and, within that we constantly work for clients on the wrong end of cyber security incidents'*

> G2P6: *'it's all about the firms internal control environment but from an information security point of view we also think about fraud so we have frameworks in place internationally to make sure we've got controls about fraud but as part of that we liaise with the information security team at the firm'*

The quotes suggest that for participants to see cyber security as part of their job role, this generally had to be identified in their specific job-related activities rather than day to day responsibility, use and compliance with policies. Moreover, participants of this viewpoint related this topic to the fact that working within a law firm meant that they all handled sensitive information, and so by nature, jobs within a law firm were particularly privy to cyber security practice. This adds to previous themes and subthemes where the data demonstrates that some participants saw law firms to operate differently from other sectors.

> FG1P4: *'I like the nature of law firms make us particularly sensitive to that kind of thing'*

A second half of participants said they did not believe cyber security to be part of their job role or referenced ways in which they indirectly interacted with technological cyber-security systems. For example, participants described sometimes 'coming across' information or GDPR compliance, and used passwords, but this was perhaps not seen as relating directly to their job requirements. As one can see below, participants would mention interactions with security, but would say that apart from these interactions their jobs did not overlap with cyber security generally or that they did not think about cyber security often.

> G1P9: *'So when I first opened my laptop I've got an encryption, so I have to and put in like a pass key and then I've got my usual password and I think every three months we have to change the password, and to be honest, I don't really think about security that much during my day to day, and in terms of information obviously, you know, I won't go to like if something says if a website comes up and says, all you should be going here. I obviously won't do that but yeah, it doesn't really come up'*

> FG7P17: *'you know emails I have to be careful who I'm sending my emails to, and the information contained in it from the clients. And apart from that there's not a lot really. I just have to monitor emails coming in.'*

These quotes and data alike often showed participants to reference small ways in which their behaviour complied with cyber-security policy, such as monitoring emails coming in.

However, it should be highlighted that although these participants did not directly say their job roles had cyber-security responsibilities, most mentioned ways in which they were compliant with policies and in this way demonstrated an element of acting responsibly. One participant mentioned that they would not say they had *'much exposure to data or cyber security except for you know, the standard so making sure that we're aware of what emails are coming in'* but '*nothing more technical than that'* (FG7P18), again perhaps highlighting the view that participants did not see human factors as much as a part of cyber security as technological factors.

This theme indicates that there was a split between participants who saw cyber security as directly part of their job role and those who did not. The group that did view cyber security as directly part of their role were mainly IT and cyber security-related participants. If participants who were part of this group were not directly IT or cyber security, they generally mentioned being involved in cyber security-related projects or referenced the need for security around client data. The second half of participants mentioned certain cyber security compliant behaviours or tools they interacted with, but in general, they did not see cyber security to be a main component of their job.

6.3 Belief of Good Cyber-Security Behavioural Practices

This theme highlights data where participants have brought up specific cyber-security policies that were then reflected on in terms of employee behaviour. In general, participants spoke about three main areas: passwords, phishing and access control. This is in line with previous subthemes on the human as perceived threats in section 5.5, as this also highlighted human factors and phishing. However, as this subtheme will demonstrate, the data presented here does align not align with in section 5.5 in terms of 'secureness', as participants perceived that they behaved well but also still understood employee behaviours and human factors to be the top threats.

This subtheme shows that participants believe their behaviours to be safe, even if they mention circumventing certain policies, and were understanding of the perceived 'toughness'

or certain policies. Participants frequently spoke about password policies within the interviews and focus groups. Participants stated that employees at the firm are required to have multiple passwords for different access points. Some participants mentioned having as many as 30 passwords, which they must change often. When participants spoke about password-changing, they generally stated they had to do this every month or every few months. Broadly, participants saw the password policies in place as secure and 'good' and believed that people complied with them. However, participants also sometimes went on to demonstrate behaviours that might not be perceived to be as secure as the policymakers would hope. For example, as the quotes below demonstrate, participants may have only changed a few letters in their password each time, had password patterns, or used the same passwords for different access.

> G1P4: *'My passwords are fairly strong. However, what I tend to do is use one password for multiple access...'*

> FG1P2: *'I would say think about passwords and try to make them secure but yeah I'm probably one of those people who is guilty of using a theme or similar combination of passwords for lots of different things yeah…'*

However, as will be demonstrated in the next subtheme on usability issues, this behaviour may be more to do with the policies themselves rather than the individual attitudes of the participants and employees more widely. Participants would often mention that they found some of the policies difficult. This was largely in reference to password policies and the number of passwords they needed to remember for security purposes.

Participants also spoke about email and phishing policies and behaviours frequently. Here participants mentioned they were given an easy way to flag phishing emails and reported that they did this often. Furthermore, one participant mentioned that employees could see if emails came from outside of the organisation, as these were flagged in their inbox.

G1P3: *'We have alerts on our emails for the things like external email so if anything tries to spoof as being internal, now it should come up as 'actually that is external' as well as an easier reporting mechanism'*

G1P2: *'You can just forward this email using a special button in a you know, like, Oh I'm flagging these phishing emails…'*

The discussions around phishing highlighted two things; firstly, phishing emails were alleged to be received often by participants and secondly, participants perceived themselves to be acting securely by reporting them. This underlines why phishing is perceived as a high threat in the previous subtheme. If such emails are being received frequently, both real and simulated, they might be perceived as a more constant threat. However, participants did feel capable of spotting and reporting such emails, demonstrated by their praise of the ease of reporting.

Access control, security techniques that regulate who can view or use resources in a computing environment, also emerged as a clear topic of conversation in the data. Participants generally mentioned that the organisation had strict access control policies in place. According to the participants, this meant that employees were not able to access any sensitive information that they did not need for their jobs and that the cyber-security team needed to approve access requests.

G1P2: *'in terms of in terms of policies or for example. I'll give you example so of course the access to the systems is restricted so not everyone not every, you just can't access specific systems with the full rights admin rights and so on and so on, right and most of the access has to be approved by the info sec team'*

One participant stated that they did not believe they had access to sensitive information, whereas others highlighted the importance of the 'confidential and personal' information they had access to.

G1P6: *'Umm I don't access a lot of sensitive data. I've got general top-level, this is the amount of profit we've earned this is the amount of expenditure'*

This quote highlights that participants potentially did not see certain pieces of information as sensitive or how they could be impacted if threat actors were able to access such information. For example, if threat actors had access to employee names, exact job titles and email signatures, could they attempt to send spoof emails pretending to be someone from inside the organisation.

Overall, this subtheme discussed security practices highlighted by participants, showing that participants spoke mainly about passwords, phishing and access control. The data shows that participants believed their behaviours to be safe, even if they mentioned circumventing certain policies, and were understanding of the perceived 'toughness' of certain policies.

6.4 Policy Pain Points

The usability of certain policies and potential pain points associated with these were also a clear subtheme in the data. Participants mentioned a few pain points, largely to do with passwords policies and access control. For example, the number of passwords they needed to remember and difficulties implementing new software. Participants presented these grievances as potential reasons for circumvention of policies. However, participants also argued that they did understand the need for such policies and were happy to comply.

A number of participants mentioned feeling 'frustrated' and saw some of the policies as 'unclear' and that processes *'could definitely be again streamlined or just made more obvious'* (G2P9). The processes participants were referring to in these cases were often access control or software approval policies. For example, one participant argued that *'there are certain business and commercial risks which one needs to take into account as well and take a more pragmatic decision on whether a particular software or solution is implemented or it's definitely ruled out'* (G1P4). This participant argued that sometimes there should be a balance

between practicality and security and used the long process it took to get Zoom approved by the security team, in order to talk to clients.

A few participants mentioned that they found information about cyber-security policies hard to find and that the system they used to find out this information hard to navigate. Other participants also mentioned that they believed things could be easier if cyber-security policies were not so stringently enforced.

> G2P11: *'I think sometimes life could be easier if we weren't in a law firm or a business that needs really tight control. And I think if things were simpler and easier to get done without having to revert back to security and infosec. I think things could be a lot quicker and smoother'*

Another policy grievance was password policies. More specifically, the frequency with which they had to change passwords and the number of different passwords they were required to have. Participants spoke about their decreased ability to cope and remember all of their passwords and the difficulty remembering passwords '*if you're asking people to do something that's wholly independent has no relationship to previous password every time' (G2P3)*. One participant mentioned they found this particularly difficult as they *'were getting old'* (FG1P1).

> FG1P4: *'Yeah, and I frequently forget, work alone is twenty thirty passwords for different access the different sites and they success with my day-to-day job and yeah it's difficult to remember them all.'*

Some participants mentioned that the number of passwords they had to remember, a combination of work and personal life, meant that they were forced to record passwords, and that they believed recording passwords *'creates a security risk'* (FG2P3). For example, one participant expressed concerns around this risk of leaving their book that they recorded passwords in along with their laptop on the bus.

> FG7P17: *'that's the problem for me as well, because I noticed that when I have complicated passwords I would write them down or tend to write them in the front of*

a book or the back of a book and then I think, 'what happens if I'm on the bus and leave laptop on the bus and I've got that book on me in my bag then they can basically get access to my laptop and know the password' so it's just harder especially changing it every now and again as well it's hard yeah.'

Despite this, participants mentioned that although they have heard that grievances with policies have led to circumvention, this was *'probably the exception rather than the norm'* (G2P9).

Moreover, many participants seemed to be accepting of the policies and said they knew they had to be strict and that they were the safest way forward, or at least stated that this was the case. This suggests that some participants were willing to understand and go along with security policies, even when they perceived there to be issues with them.

FG3P5: *'I haven't got a problem with any of the policies yeah. I think they're in place for a reason and we should adhere to them, we understand why they're there now more than before so yeah.'*

G2P9: *'I completely understand why these* [policies] *are in place, but it can take quite a long time to resolve and get ultimately what you need to be done yeah. If that makes sense?'*

FG4P8: *'…it is annoying to remember so many passwords especially when they should be different to your personal passwords, but yeah. I think it's the safest way.'*

This subtheme demonstrates that participants perceived certain usability issues and pain points with some security policies. For example, some participants perceived getting approval for new software to be a long and complicated process and highlighted a need for a balance between security and practicality. Other participants emphasised issues with password policies, specifically the amount they had and the frequency they needed to change them. Participants demonstrated how such password policies could lead to further security risks, such as writing passwords down in a notepad they carried around along with their laptops.

Despite these anecdotes, many participants displayed understanding and acceptance of these policies and were willing to adhere to them in the name of security.

6.5 Mixed Views of Awareness Training

This theme highlights data surrounding participants' thoughts on the cyber-security awareness training that they were given prior to the time of data collection. Participants largely spoke about the training they received when they initially started their job, which some participants mentioned was refreshed yearly and phishing tests that they received. There were varied views on the effectiveness of the training, but generally, participants viewed the training they received as good.

The training was often described as good and impactful. Induction courses were said to involve a range of cyber-security topics and that they received web-based training material that they could access later on.

> FG7P16: *'It's pretty good training really. I think when a new starter is to join it's certainly used to be exciting, I used to be in the training team. We did an induction which incorporated various things and it was certainly what about introduction to the IT systems and how to log in and how to connect with the VPN. And then in addition to that, I think there's a web-based training material which is compulsory for information security. Is that right? I think that's correct.'*

Additionally, participants mentioned finding posters and emails the cyber-security team sent out to be helpful and something they did read. For example, one participant mentioned reading about cyber-security attacks that were happening around the world to be helpful (information they often received via email from the information security team). Phishing testing was also something participants mentioned regularly experiencing within the firm.

> FG6P12: *'Not phishing emails but pretend phishing emails and we've got to spot them a report them.'*

FG6P13: *'there's the continuous sort of fake phishing emails sent out to see who can spot them, it's kind of an ongoing thing really.'*

G1P8: *'they're usually fairly obvious, in that they're not and not something that you should be looking at or clicking on, and so I think it's worthwhile doing just so like you say people can and have that confidence to report things yeah and, when they do come up and it's not a test'*

The firm's phishing simulations were generally perceived to be harmless and a valuable exercise for employees to undertake by most participants who mentioned the phishing tests. Participants argued that they were not difficult. A few participants mentioned being caught out the first time or one of the times that these emails had been sent around and mentioned they had not clicked on a link since and suggested that maybe the training had *'done it's job'* (FG1P4). One participant said that phishing tests had helped him and a colleague. Others highlighted that the tests helped them keep cyber security at the front of their mind and were clear demonstrations of how cyber-security threats work and raised awareness of what they can expect if they were to receive real phishing emails. Phishing testing was also something participants mentioned regularly experiencing within the firm.

The positive views of phishing tests were perhaps related to the way they were dealt with by the cyber-security team. In the elite interviews the two participants mentioned that they only reported the success of the phishing tests and not the failures, and that this sentiment fit into a wider narrative of trying to push the idea of the human as a solution to cyber security, rather than a hinderance.

EI1: *'also being very positive in terms of when we have a phishing campaign and we have to report on that, we will report on the success of it not the failure of it. Yeah. So 74% have identified have, not fallen so that shows a certain amount of resilience. And that's all part of the narrative which we want to talk to the board about, to see security is a positive thing not a negative thing.'*

Many participants argued that they had enough training and stated that they did not require anything further as this might overwhelm them, or that they simply did not want any more training. Some participants also expressed concern that too much more training could lead to a loss in effectiveness of the message.

> G2P8: *'Hammering home messages I think you know, you run the risk of, if you keep trying to make noise, it ends up becoming sort of background I suppose or you lose the effectiveness of your message if you just keep banging the drum.'*

However, many participants did also perceive potential problems with the training. A few participants saw the training as not impactful and some had suggestions for ways it could be improved, whereas others could not pinpoint when their last training had taken place.

> FG5P10: '*I probably would like to do something a little bit more in-depth on a personal note, but other than that and I'm pretty comfortable.'*

> G2P8: *'Yeah, like I say that there are emails that go around and not regular regularly could probably do them a little bit more often just to keep it kind of at the front of everybody's mind'*

One participant also highlighted that the degree to which training was good and impactful depended on the individual person and how they engaged with it, arguing that there was only so much training the firm could put forward. The rest, the participant argued, would be down to the individual.

> FG6P13: *'I think the only thing would be is how it an individual engages with the training that we're provided with, I suppose that the firm can do so much, but it's down to the individual as to how much they actually take on and practice yeah in like the day today work.'*

Another participant argued that they did not find security content to be engaging, and was not a very interesting topic, which reduced their interaction with the topic.

G1P9: *'E-Learning courses are just so boring. I just feel like that's not the way to get people to. I wouldn't have another alternative but I just think just trying just getting people especially so obviously we work out a law firm so the fee owners especially because there are times always billed.'*

However, this participant also stated that they would not want any other alternative training either. Other participants had specific suggestions on how training could be added to and improved, which provided useful insight for creating future training programmes. Participants here argued that content could be more personal to employees and also give real examples of experience and implications of cyber-security risks. A few participants also highlighted that they would prefer face-to-face training over that done online.

G1P1: *'I think it's that if people could actually experience what some people are going like have to go through and in this respect, if you lose stuff if suddenly stuff gets like kind of corrupted, and You know what I mean, in terms obviously there are so many implications to try to do something like that yeah it probably I think that maybe a step too far but ultimately for me, that's the way that it would make it real for everyone yeah.'*

In summary, this subtheme demonstrates an array of perceptions about the cyber-security awareness training employees received at the firm at the time of writing. Many participants described the training as good, finding exercises such as fake phishing emails useful. A few participants argued that they did not see the need for any additional training. It was also clear from the data that there was no recalled consensus on what training employees within the firm received. Other participants provided suggestions of ways the training could be improved for them, such as including more detail and making communications more personal.

6.6 Summary

This high-level theme included four subthemes looking at various aspects of policies and training within the firm and the participants' thoughts and behavioural practices surrounding these expressions. When considering possible threats, participants largely spoke about client-related risks, phishing and human behaviours as their top concerns and did not highlight any technological factors. There was a split between participants who saw cyber security as directly part of their job role and those who did not, and this seemed to be influenced by whether they worked in IT-related roles. Participants also perceived specific usability issues and pain points with some security policies. For example, some participants perceived getting approval for new software to be a long and complicated process and highlighted a need for a balance between security and practicality. Lastly, the data highlighted that there were many differing views about the cyber-security awareness training employees received at the firm. This chapter highlights the nuances of how policies and training work and are perceived within the context of a single organisation.

6.7 Discussion

This discussion synthesises and grounds the findings from this chapter within the research and theory discussed in the literature review section. This the discussion will look at the behavioural practices of employees in the context of such perceived threats, perceptions of job role, and pain points with policy, relating this to previous usable security research (Beautement & Sasse, 2009; Inglesant & Sasse, 2010; Nurse et al., 2019a; Weirich & Sasse, 2001) and theories such as PMT (Prentice-Dunn & Rogers, 1986) and the EPPM (Witte, 1996). Lastly, the cyber-security training within the organisation, as experienced by employees, such as perceptions of phishing tests used by the organisation, will be discussed in relation to previous literature (Kumaraguru et al., 2009; Kumaraguru et al., 2007; Sheng et al., 2010).

6.7.1 Responsibility

Firstly, the current section's findings demonstrated a split between participants who saw cyber security as directly part of their job role and those who did not. The group that viewed cyber security as directly part of their role contained mostly IT and cyber security-related participants. The second half of participants who discussed this topic mentioned certain cyber security compliant behaviours or tools they interacted with but, in general, did not see cyber security to be a main part of their job. This might then help understand non-compliance within the current research as well as speak to research within the literature looking at the impact of perceptions of responsibility on compliance. In the literature, it is argued that high levels of responsibility are a precursor to high levels of compliance (Blythe et al., 2015; Filipczuk et al., 2019; Hadlington, 2018; Kim & Han, 2019). If participants in the current organisation do not see cyber security as part of their job, this might mean they feel a reduced level of responsibility. This finding, along with the finding from Chapter 5 that participants believe cyber security to be managed for them, also supports previous research showing that individuals are devolving responsibility for their cyber security to technical interventions and senior management (Tischer et al., 2016). Moreover, the current research shows that security professionals and non-security related employees have different ideas surrounding responsibility (Posey et al., 2014). The present findings add to existing research by showing that those in IT roles may also possess similar ideas as those in security roles. However, it may also be that participants in the current study were talking about their job role in a more literal sense and may understand any cyber-security behaviours they partake in to be behaviours that go above and beyond their job role.

The TPB (Ajzen, 1985) may also offer insights into how responsibility and related concepts might interact with individuals' intentions to behave according to the cyber-security rules and policies that apply to them. TPB proposes that the intention to perform a specific behaviour can be predicted accurately by three kinds of considerations (Ajzen, 1985): behavioural beliefs, normative beliefs and control beliefs. Normative beliefs refer to the possible expectations of other individuals and one's motivation to fulfil these expectations. In the current research, we can see that individuals may not believe they expected to have a high degree of responsibility for cyber security, as seen by the discussion around cyber security being managed for employees, along with the understanding that cyber security is not part of their job role. The theory would suggest that if the subjective norm is not favourable, this

might reduce the likelihood of employees performing recommended cyber-security behaviours (Ajzen, 1985). This then adds to findings in the current research within previous chapters, where elements of data related to control beliefs and perceived behavioural control concepts within TPB. Moreover, these findings together extend previous examinations of the TPB in relation to cyber security by offering support for its concepts within qualitative data in the context of an organisation (Bulgurcu et al., 2010; Ifinedo, 2012; Kim & Mou, 2020; Sommestad et al., 2015).

6.7.2 Usability Explanations: Psychological Theory and Usable Security

In general, participants demonstrated a belief that behavioural practices within the organisation were good, but also went on to name some examples that would likely be considered not best practice. For example, participants mentioned password behaviours that could be considered to be undesirable, such as only changing a few letters in their password each time, having password patterns, or using the same passwords for different access points. The current research supports previous studies that have demonstrated that employees may frequently report policy issues, such as authorisation operation issues, despite a high level of overall reported compliance (Bartsch & Sasse, 2012). In this previous study, policy issues sometimes lead to circumvention of access control systems, such as sharing access passwords with co-workers or technological circumvention, such as sending documents via different means (Bartsch & Sasse, 2012). More broadly, the current findings relate to the surrounding literature by showing that employees are not always compliant (Blythe et al., 2015; Herath & Rao, 2009; Ifinedo, 2009; Siponen et al., 2010; Vance et al., 2012). This finding is longstanding within cyber security, and the current research does not assist the current dialogue by demonstrating that employees may not always be compliant with policy. However, current research can add to usable security research by seeking to understand, by applying theory and research, why this might be the case. In the current research, participants noted many different pain points regarding security policies. Participants spoke about difficulties with password policies, access control, software approval policies and problems with finding information on policies and what to do if something related to cyber security were to go wrong.

Usable security research and dialogues offer explanations here, as many of the behaviours mentioned, such as reusing password policies, may also be due to unusable policies. For a few decades, researchers have argued that password policies are often too challenging and make compliance with policies difficult, as well as reduce levels of productivity (Beautement & Sasse, 2009; Inglesant & Sasse, 2010; Nurse et al., 2011a; Weirich & Sasse, 2001). Research has concluded that users are, in general, concerned with maintaining security (Inglesant & Sasse, 2010), but existing security policies are too inflexible and difficult to match user capabilities (Beautement & Sasse, 2009; Inglesant & Sasse, 2010; Nurse et al., 2011a; Weirich & Sasse, 2001). Therefore, password policies place demands on users, which negatively impact their productivity and, ultimately, negatively impact their organisations by creating security problems of their own (Inglesant & Sasse, 2010; Kirlappos et al., 2013). The current research demonstrates that employees still believe password policies to be difficult to manage.

Moreover, participants mentioned that it was also necessary for them to remember a variety of different passwords in their personal life beyond work. This further demonstrates that organisations need to consider the context in which individuals are being asked to remember passwords. As although organisations may not believe their policies to be a strain, they need to consider other pressures that employees might be experiencing. It was also clear that participants still intended to comply with policies with which they had pain points. This suggests that any issues arising from policies are to do with the usability and not employees' intention to comply.

PMT offers insights into the consequences of policies that have reduced security usability. As part of the mental calculus suggested by PMT (Prentice-Dunn & Rogers, 1986), individuals who find intrinsic and/or extrinsic benefits from purposely not performing protective actions against threats or for responding in a maladaptive fashion may be less inclined to perform the behaviour (Posey et al., 2014). Therefore, protection motivation is a negative function of any perceptions of rewards of maladaptive responses and the possible costs of the suggested adaptive behaviour (Norman et al., 2005). In this way, PMT can be seen to complement usable security work by suggesting that if employees see the benefits of not complying with

policies, they will be less inclined to do so (Inglesant & Sasse, 2010; Kirlappos et al., 2013). In the current study, participants saw some security policies to be a long and complicated process and wanted a balance between practicality and security. It could be argued, therefore, that participants might be less inclined to perform the behaviour as a possible reward for non-compliance would be saving time (Pham et al., 2017). Vance et al. (2012) detected that the cost of compliance negatively influenced employees' compliance intention, as employees considered the inconvenience of following cyber-security policies a legitimate reason for not complying with such policies. Therefore, this finding lends support to previous research demonstrating the impact of response costs on cyber-security perceptions and behaviours (Floyd et al., 2000; Tsai et al., 2016; Vance et al., 2012) by finding qualitative examples of such concepts in the context of an organisational case study. However, previous findings have been mixed, with one study showing that while response efficacy and self efficacy were found to have a direct and significant impact on cyber-security compliance intentions, response cost did not appreciably contribute to predicting compliance intentions (Herath & Rao, 2009a). The current research cannot say definitively that response costs influence compliance but offer support for the possible existence of these concepts in context.

The TPB's (Ajzen, 1985) concept of behavioural beliefs may also offer insight into the consequences of poor policies here. Behavioural beliefs within TPB refer to beliefs about the probable outcomes of the possible behaviour and the assessments of these outcomes. If an individual perceives a behaviour to have adverse outcomes, such as a cyber-security behaviour reducing productivity, this might reduce their behavioural intention. This theoretical application offers further insight into why usable security and usable policies are so important, with usable security research supporting the importance of behavioural beliefs. Cyber-security policies and systems that do not significantly factor in security usability place demands on users, which impact negatively on their productivity and, ultimately, that of the organisations in which they work by creating security problems of their own (Inglesant & Sasse, 2010; Kirlappos et al., 2013). Of course, seeing the benefits of non-compliance will not be the only factor influencing employees to behave in a certain way, but research has demonstrated it to be a contributing factor (Koppel et al., 2015; Tam et al., 2010).

6.7.3 Phishing and Training

Researchers within usable security and the wider HCI literature have been critical of phishing tests (Kirlappos & Sasse, 2011; Kumaraguru et al., 2009; Kumaraguru et al., 2007; Sheng et al., 2010). These criticisms have related to both the ethics and efficaciousness of the metric. Phishing one's own employees may reduce trust by making it seem to employees that their organisation is tricking them. Moreover, it can be stipulated that the metric does not have validity in that it may not be measuring what it claims to be. For example, the measure might not be measuring employee ability but rather the style and mastery of the phishing emails. Therefore, it has been argued it would be more useful to look at why employees might fall for certain phishing emails over others. The current research does not contradict such claims. However, in the present case study, employees generally perceived the firm's phishing simulations as a useful exercise. Employees did not mention any negative implications and did not see the exercise as a test. Others highlighted that the simulations helped individuals to keep cyber security in mind and raised awareness of what they could expect if they were to receive real phishing emails. This then extends the existing narrative surrounding phishing your own employees (Kirlappos & Sasse, 2011; Kumaraguru et al., 2009; Kumaraguru et al., 2007; Sheng et al., 2010) by suggesting that employees in certain circumstances do find the exercise useful and that they help increase awareness and knowledge.

It was also suggested within the elite interviews that the phishing tests conducted by the firm were conducted with the intention to be positive, whereby the firm reported the success of phishing attacks and did not use sanctions to discipline employees. This method of phishing campaigns may therefore negate some of the negative ethical implications highlighted by researchers (Kirlappos & Sasse, 2011; Kumaraguru et al., 2009; Kumaraguru et al., 2007; Sheng et al., 2010), as employees may not feel their trust has been impacted if the data is demonstrated positively. Recent research has revealed that organisations use a variety of rewards and sanctions with regard to cyber-security behaviour campaigns, such as phishing simulations, with sanctions being used in some form across 90% of the organisations studied (Blythe et al., 2020). The present case study, therefore, highlights the benefits of an organisation which does not use such sanctions and has perhaps allowed employees to see

the positive implications of phishing tests. Previous research more broadly has shown that, rather than be motivated by rewards and sanctions, individuals within organisations are much more likely to name intrinsic motivations for compliance with cyber-security policy, such as organisational commitment and personal pride (Posey et al., 2014). Chen et al. (2018) found that complying or not complying with the cyber-security policy is based mainly not on formal sanctions but on informal sanctions and efficacy. Moreover, by making phishing campaigns positive, reporting the wins and not failures, the organisation would arguably boost employees' efficacy by showing that they are capable and able to spot and report phishing emails. The current research, therefore, adds to this previous research by demonstrating that phishing campaigns, when they are used positively without sanctions, may be viewed positively by employees.

In addition to findings related to phishing campaigns, participants in the current study also offered insights that may be useful to cyber-security professionals and researchers. First, it is noticeable that participants in the organisation offered an array of differing opinions regarding the usefulness of training. This supports previous research, which suggests individuals respond to cyber-security training and campaigns differently (Berris et al., 2015; Johnston & Warkentin., 2010). Participants in the current study argued that content should be more personal to employees and give real examples of experience and implications of cyber-security risks. Suggesting that in order for organisations to have usable training, information should be tailored to individuals and not be uniform across an organisation. Employees, after all, may have different levels of knowledge and have different cyber security requirements based on their job roles. This is further supported by findings in the previous chapter, where participants argue that fee earners and support staff behaved differently due to their roles' differing natures. Moreover, this finding supports the idea that organisations should invest in methods and tools that facilitate systematic feedback from users (Reinfelder et al., 2019), as this would help them gain insight into the mindsets of their employees. Hence, enabling organisations to assist employees with cyber-security behaviours more effectively.

Other participants stated they did not want any additional training. This statement may reflect that participants either believe they have had enough training or that the training they

have received has been sufficient in giving them the capabilities to behave securely. Participants argued that too much training could be overwhelming, which fits into a dialogue within usable security, suggesting that participants should not be inundated with cyber-security awareness training if the training is to remain effective (Sasse & Rashid, 2021). On the other hand, this could indicate a dislike of training. Previous research has demonstrated that employees within organisations find cyber-security training to be boring. In one study, aptly entitled "Get a red-hot poker and open up my eyes, it's so boring" (Reeves et al., 2021), employees had a generally poor view of cyber-security training and awareness programs. Participants in the study reported that the same factors that are important for effective non-cyber-security training are also essential for cyber-security programmes, such as well-designed workplace systems and management role modelling (Reeves et al., 2021). Haney and Lutters (2018) further demonstrated that cyber security advocates often have to overcome perceptions that security is scary, dull and confusing. To overcome perceptions that security is boring, participants in Haney and Lutters' (2018) study stated that they promote recommendations that can be realistically accomplished with usable security solutions and employ engaging rhetorical techniques (Haney & Lutters, 2018). Therefore, this study, along with the current research, again highlights the importance of promoting usability within the cyber-security context, as it can also make security less frustrating and confusing. Moreover, game-based training has been shown to be effective for cyber-security awareness and training skills, seemingly providing engagement and entertainment as well as teaching cyber-security concepts and practices (Cone et al., 2007; Cone et al., 2006). Based on the current and previous findings, future research needs to look at testing awareness and training methods that are viewed more positively by employees and tailor such methods to more individual outlooks.

6.7.4 Conclusions and Contributions

In summary, this discussion demonstrated how and where the findings could be related to the existing usable security research and deepened by psychological theory. It was shown that the focus on human factors as threats in the current data lends support to previous work (Schaik et al., 2017) and that this perception, according to PMT, might reduce efficacy in

individuals. This idea is also a possible example of the availability heuristic (Tversky & Kahenman, 1974), a previously proposed heuristic within cyber security that has not yet been empirically demonstrated (McAlaney & Benson, 2020; Tsohou et al., 2015). Ideas concerning job roles were also related to previous research suggesting a split between ideas of responsibility between cyber security and IT professionals and other non-security roles. This was then related to the concept of normative beliefs within the TPB. Given the findings related to behavioural practices, along with the discussion of policy pain points, the findings were also related to the usable security literature (Beautement & Sasse, 2009; Inglesant & Sasse, 2010; Nurse et al., 2011a; Weirich & Sasse, 2001). Based on this discussion, it was suggested that organisations not only look at the impact of organisational cyber-security policies and their usability on employees but also how policies and cyber-security requirements in people's personal lives. For example, how many websites require different and complicated passwords. PMT and TPB were used here to offer insights into the consequences of policies that have reduced security usability and to aid understanding of how this might impact employees' cyber-security perceptions and behaviours. Finally, the participants' perceptions of cyber-security training were discussed. It was demonstrated that future research should look at how cyber-security training might be best tailored to fit different cyber-security needs and further demonstrated the usefulness of organisations creating feedback and dialogue with employees.

Chapter 7. The COVID-19 Pandemic and Remote Working

7.1 Introduction

As discussed in the literature review and methodology chapter, this research took place during the COVID-19 pandemic, with the data collection, taking place between March-August 2020. The impact of the pandemic on a number of research topics, such as the various aspects of cyber security, is a new research area that is being constantly updated as the pandemic progresses through its different phases (Lallie et al., 2021; Monteith et al., 2021, Wang & Alexander, 2021). In this case study, the data collected on the impact of the pandemic was, therefore, largely incidental and opportunistic. The data provides contextual observations by participants about their ongoing experiences of remote working and the possible impacts on cyber security. This theme is separated from the rest of the chapters because the findings here relate to participants speaking directly about the pandemic or the ramifications of the pandemic. Although all data collection took place during this time, and within this context, in the previous chapters, the participants were drawing on perceptions and knowledge that also existed outside or before the pandemic began.

Therefore, in this chapter, the research findings concern the subthemes identified through the data analysis that relate to remote working during the pandemic. The first section focuses on participants' preparedness with respect to security during the pandemic, while the second engages with participants' notions of risks in the context of home working. Section three centres on the impact of working entirely online, and Section four highlights the distinctions between personal and organisational risk. This chapter will then discuss the findings presented in the context of the broader literature and theoretical framework. The discussion will cover recent and emerging research on the impact of the pandemic on cyber security and workers, as well as previous research on usable security and psychological theory.

7.2 Feelings of Preparedness and Security

At a high level, this theme suggests that participants felt that their organisation was relatively prepared for the move to remote working and that there was little change in terms of cyber security from the office to remote working. Participants gave a variety of reasons for this, for example some participants mentioned that the firm had previously set out clear working from home policies, whereas others suggested that the 2017 cyber-attack had prepared them in that the attack had also imposed a period of uncertainty and remote working.

Many participants felt that their employer was prepared for the move to home working -- this also included them feeling secure and supported in the move as the organisation had been previously set up for their employees to work flexibly, i.e., from the office, home, and while travelling. This included the fact that lawyers had laptops that they were already able to take home. This meant that much of the technology and cyber-security systems, although not at the scale needed during the pandemic, were already in place. Participants compared this to other industries that were not previously set up to work remotely, such as the education sector.

> G2P10: `*Yeah, I think it was more geared up to the fact that you know we're a pretty mobile and capable workforce anyway, you know, most of our lawyers have requirements, that they had before lockdown, to travel and work remotely. So, we had the systems and the tools. Most of our lawyers had laptops, for example, so we were pretty well geared up to be able to facilitate that remote working'*

A few participants also hypothesised why working from home and flexible working policies were in place previously. For example, some participants referenced the cyber-attack in 2017 and how it encouraged the firm to improve its cyber-security policies and created an understanding of the ease of mobilising the workforce within the firm to work from home. This again adds to the possible positive impact of the 2017 cyber-attack on the firm's human element and cyber-security practices, although, in this case, a completely unforeseeable one.

FG1P2: *`Yeah I think the cyber-attack in 2017 at not only made them change cyber security but made them think about how easily can we mobilize people.'*

FG1P2: *'And that's probably very similar to having all your staff working remotely at a moment's notice, and was never really contemplated in a lot of businesses, and they then found themselves in a situation where they just simply don't have the resources to do so.'*

Similarly to feeling prepared, some participants felt there had been no change in the cyber-security risks associated with working from home, apart from changes in the convenience of doing certain tasks such as connecting to the server, which was automatic when situated within the office.

G1P5: *`I feel exactly the same as if I were in the office because I've still, nothing's changed in terms of, it's literally just where I am physically that's changed nothing has nothing else exchanged apart from the way that I said that I connect to the server now...'*

Participants also noted that they felt secure working from home and supported by the IT and cyber-security department and that this period proved the firm's ability to function remotely. IT and cyber-security departments were still able to support employees effectively from home by providing access to systems and making employees feel a sense of security.

FG5P11: *`I find I am very really supported by IT and it's been really smooth working from home and we've had so much support with our equipment and what to do and so I've found it all quite easy to set up at home, yeah and I find that IT very helpful and easy to access and if I have a problem they're always there.'*

G2P1: *`The lock-down has helped with that because now pretty much everyone's been forced to work from home they've all realized that actually quite easy to do.'*

Therefore this theme largely suggests that many participants felt prepared and secure in the move to remote working, mainly because previous remote working practices meant the organisation had existing policies in place.

Another minor theme of preparedness was the discussion of awareness campaigns for home-working employees. Participants generally stated that they received information on cyber security in the home in the form of emails from the organisation as well as information on how cyber criminals might use COVID-19. Participants stated that cyber-security information was given regularly and in an *'easily digestible'* (FG1P2) way. For example, participants received information on not taking physical papers from the office to home, printing anything confidential, and not using personal email accounts to send or receive scans.

> FG1P2: *'we had quite a lot of communication coming out about getting an IT set up and also about how to handle cyber security when working from home...'*

> FG4P9: *`I think we do get emails about it there was one about and working safely from home during coronavirus so I think they do they do push emails about cyber security. I feel like they do quite frequently.'*

However, participants in the elite interviews, EI1 and EI2, stated that the pandemic had made their roles in delivering training and awareness and EI2 stated that in general '*COVID has definitely made things a lot slower'.*

This subtheme demonstrates feelings of preparedness and support in terms of cyber security while participants were working at home, from the cyber-security team and the wider organisation. Furthermore, this demonstrates the possibility of remote cyber-security awareness campaigns, as participants perceived that they had effective cyber-security communication about working from home.

7.3 The Remote 'Risk'

Although the previous theme highlighted feelings of security, participants also mentioned perceptions of cyber-security risks associated with working from home. For example, participants mentioned that individuals might be more relaxed at home and, therefore, perhaps pay less attention to cyber-security policies. Moreover, this theme highlights how participants perceived the main 'risky' aspects of remote working were those to do with the physical and human elements.

In general, when talking about the risks of remote working, participants referenced living situations and the environment in the home being more relaxed than that of an office environment. Many participants lived with friends, partners, or families, citing the possibility of accidentally sharing information with them as a possible risk. However, it should be noted that most participants stated that many employees lived on their own or were particularly careful to not share information with those they lived. Other participants suggested that they did not work with any 'secret' information or mentioned a level of trust between those they lived with and themselves.

> G1P6: *'I know that I've shared my space with my husband who's in a completely different line of work. And I've had some quite confidential phone discussions, he only hears one side and I'm not really the person contributing this top secret information so I don't think any company's secrets of leaked out.'*

> FG1P1: *'If you're living with flatmates that you maybe don't know as well and you don't trust the same way and there's a chance that someone's looking over your shoulder and looking at your password or and I would say the threat in that perspective comes from a much more physical being on the phone talking about clients and rather than by virtue of having to have a laptop at home with you and be emailing from home...'*

One focus group participant mentioned a potential issue for junior lawyers who could be living with competitors or those working on the opposite side of a particular case.

FG7P15: *'we might have trainee lawyers sharing flats with people they were at uni with that might work for competing firms for example, so they might be you know quite curious as to what our lawyers are working on when they could be working on the opposite side for example'*

This was also echoed in the elite interviews, where it was noted that a possible consequence of working from home was the potential for employees to share confidential information inadvertently.

EI1: *'When people live in a shared kind of household and are always having sensitive conversations, they need to find a safe place away from listening devices like an Alexa and Google home where they can have confidential conversations and I suspect lots of lawyers are either married to other lawyers or are sharing accommodation with other lawyers who work for different firms yeah, so we've got those kinds of things where actually it's just about situational awareness try the kind of get it to the front of the minds of those individuals.'*

Participants also mentioned that individuals might prioritise efficiency over security when working from home compared to the office, the possibility that individuals *'will become a little bit more relaxed'* (G1P4), or even complacent, owing to the fact that they perhaps feel an increased element of safety in their own homes. However, participants did not expand much on why they believed this to be the case.

FG3P7: *'Yeah, I think it's the same most of the time, I think sometimes people get complacent when they're at home and they think well, I'm relatively safe here...'*

Participants argued that this had considerable potential for reputational damage to the firm, which relies on its reputation with clients to function. This was also spoken about in relation to the problem of printing and shredding confidential information at home.

FG7P15: *'Not having the opportunity to shred documents properly and printers, because the equipment isn't there… they might take shortcuts if the you know,*

especially in the early days, when we weren't set up fully as securely as we could be from the off that you know people are under time pressures with clients and things'

EI1 and EI2 also noted that the firm had noticed an increased number of opportunistic phishing attacks that used COVID-19 as a ploy. Hence, participants would be receiving these phishing emails in their home environment. A more significant problem since participants stated that individuals might feel more relaxed at home or if they were feeling stressed from the pandemic.

EI1: '*There's obviously being a huge uptake in COVID based attacks yeah and I let the firm know about kind of covid scams covid phishing attacks. The use of kind of government or these ordinary NGOs to kind of use as a front for these attacks…'*

This theme, therefore, highlights that when speaking of the risks of working from home, most participants referenced the physical and human-related risk factors, mainly related to the physicality of being in the home environment around others who do not work for the same firm.

7.4 Missing Face-to-Face Contact

Despite feelings of preparedness and security, as noted in the first theme, participants also spoke about missing face-to-face contact with colleagues and how this impacted their work-life experience. This was a slightly smaller theme in the number of participants who referenced the issue, perhaps because participants understood the focus of the research to be on cyber security. However, it was still prevalent.

G1P2: *'the only thing I'm missing is it's maybe you know this the social aspect of that right'*

It was highlighted that the lack of face-to-face contact made some organisational processes more complicated, that it was more difficult to ask someone a question when needed, and

that this could be an added risk. There was, therefore, a different sense of invading someone's 'space', taking up too much of their time, or it being a less casual conversation when asking someone a question remotely compared to asking someone face-to-face.

> G1P8: *'Yeah, I've always think that and a little strange because my team is very small anyways, but and working remotely it's been kind of hard because you don't want to be calling the same person constantly and because you're a small team, whereas you just have a chat across the desk, you can't do that in the same way so I think it is different not having a person right next to you to bounce query of and, It's definitely different'*

Participants mentioned that this lack of ease in asking questions meant that they would only query larger issues they were experiencing. Additionally, participants mentioned that they missed the social aspects of this office, feeding into the wider question of employee wellbeing in remote environments. One participant also highlighted the difference in onboarding during the pandemic. This participant had never met anyone from the office and only met their manager 'on the interview back in February' (G1P2). This was seen to have made it harder learn their new role.

Furthermore, EI1 mentioned feeling a broad sense of pressure caused by the pandemic and having to work from home, a sentiment they believed was shared by other employees.

> EI1: '*A guilt of not being able to do their job to the best abilities not being able to homeschool their kids to the best. Feeling that they're not delivering on all the fronts as best as they can, but what I think, those people don't appreciate it we're all feeling that thing they're not alone in that guilt. I feel terrible that sometimes my wife is having to stop her work to help schooling or something. I'm having to stop my work and yeah'*

This subtheme steers away from direct impact on cyber-security perceptions, awareness and behaviour. The data here highlights how possible feelings of being more isolated impacted participants and how it made work, and perhaps complying with organisational policy, more

difficult. This data is relevant to the data on the impact of cyber security, as employee mindsets significantly impact how they work and interact with organisation policy.

7.5 Summary

Overall, the data within this theme demonstrated how the organisation and its employees were impacted by the global events continuing to this day (at the time of writing). Although, at the time of data collection, the duration and later impacts of the pandemic were unforeseen. This data showed that employees felt their organisation were uniquely prepared for the move to remote working, even though the pandemic had been unpredictable. However, participants also highlighted some potential risks that remote working and the pandemic created, such as privacy between partners in the home environment. Lastly, participants also highlighted some difficulties surrounding feelings of isolation and how this may impact their ability to work efficiently.

7.6 Discussion

This section will look at how participants viewed the move to remote working during the COVID-19 pandemic and, in turn, their influence on participants' feelings towards the organisation and cyber security adds to the current literature on COVID-19 and cyber security (Crossland & Ertan, 2021; Furnell & Shah, 2020; Lallie et al., 2021; Wakefield, 2020; Weil & Murugesan, 2020). Previous research has highlighted that organisations were wholly unprepared for the shift to remote work (Georgiadou et al., 2021; Lallie et al., 2021), whereas the current findings show evidence of preparedness within the organisation. However, the feelings of isolation felt by participants are supported in the related literature (Khan et al., 2020; Lallie et al., 2020; Serafini et al., 2020; Xiao et al., 2021). Moreover, this discussion section will discuss how the findings related to the COVID-19 pandemic and the move to remote working can be viewed through the psychological lens of PMT, the EPPM and the TPB.

7.6.1 Preparedness

The findings showed that the participants generally felt prepared when moving from office-based to home-based or remote working. However, broader research has hypothesised and highlighted how employees and organisations had experienced a sense of unpreparedness in this move, mainly due to the speed and scale with which it had to be done (Crossland & Ertan, 2021, Georgiadou et al., 2021; Lallie et al., 2021; Nurse et al., 2021). In the study conducted by Georgiadou et al. (2021), more than half of the participants reported that they were not briefed about work from home security. Other papers point to this as an example of security risks likely to be rife in times of remote working (Nurse et al., 2021). This may become an issue again when and if the workforce moves back to offices, where a different set of behavioural practices are perhaps required (Crossland & Ertan, 2021). Participants, who may have been working remotely for over two years or still be remote working at the time of writing, may need to be refreshed on office-related cyber-security practices, which will likely differ from remote practices. This change could be further convoluted by hybrid working patterns that many organisations have adopted.

For the participants in the current study, the security risks related to remote working were not perceived to be noticeably different to those experienced when working from the office. Many participants also linked pre-existing cyber-security policy with their sense of preparedness for remote working. However, participants did not reflect on the organisation's technological preparedness. This is partly a result of the focus of our study and suggests that for employees, the behavioural aspects related to security were foregrounded. However, the current findings contrast existing work on organisations' (un)preparedness for remote working at the scale experienced during the pandemic. For example, working from home required many employees to work with new third-party communication tools with which they had no familiarity. Some organisations also did not have the required technological security infrastructure to support employees working remotely. The literature suggests this has, in some cases, had a critical impact on an organisation's security, partly because the time needed to acquire, set up, configure and update secure devices for employees to an acceptable threshold was very limited (Georgiadou et al., 2021). Limited resources to invest in secure VPN connections for remote employees, secure devices, and home Internet

connections in a short amount of time have also been highlighted as an underpinning factor in some employees and employers feeling unprepared for security during the pandemic (Lallie et al., 2021).

Other research has indicated that working from home and using personal devices significantly increased the potential security risks during the pandemic (Chigada & Madzinga, 2021). Moreover, according to Lallie et al. (2021), the software vendors that provided software solutions conducive to work from home and remote communication were themselves unprepared in terms of the security of their products. However, for the participants in our study, increased security risks related to working from home centred on `human risks' rather than technological risks. The discrepancy between the literature and the findings from our study regarding feelings of security and preparedness thus suggests pressing questions for research in terms of cyber security. Finally, Razif et al. (2020) suggest that the `availability of infrastructure, facility and technical support is of utmost importance when planning for remote working. These factors, along with effective leadership and training, are seen to underpin the level of working from home technology acceptance experienced by both employees and organisations.

Findings also highlighted that some participants in the current study believed the previous cyber-attack in 2017 to of unwittingly helped their firm prepare for the move to remote working during the COVID-19 pandemic, as similar remote working policies were put in place before. This, therefore, extends previous research looking at the impact of cyber-attacks on employees and organisations. Previous studies and research highlight the physical, digital, economic, psychological, reputational, and social harm often caused by cyber-attacks and demonstrate real examples of when this has been the case (Agrafiotis et al., 2018; Bada & Nurse, 2020). The current research adds to this by showing that on top of all of the harm that cyber-attacks may cause, organisations that manage to go through this and come out the other side may retain some resilience against similar situations requiring quick movement and cyber-security policy changes. This is, of course, by no means a suggestion that suffering a cyber-attack is by any means something to aspire to happen. However, it does highlight the possibility for firms to apply learnings from such situations to other aspects of a business. Perhaps, for example, if and when organisations post-pandemic suffer cyber-security attacks,

they will be able to mobilise their workforce more efficiently owing to previous remote working strategies and policies.

Beliefs concerning preparedness have been related to PMT (Prentice-Dunn & Rogers, 1986), the EPPM (Witte, 1996), and TPB (Ajzen, 1985) in wider literature outside the realms of research on COVID-19 and cyber security. Generally, feelings of preparedness and participation in preparedness behaviours are seen as a good outcome within PMT, EPPM and TPB models when attempting to encourage people to prepare for a particular risk-related event, with these models having been demonstrated to be predictive of such behaviour (Mulilis & Lippa, 1990; Tan et al., 2020; Tang & Feng, 2018; Weber et al., 2018). This could suggest that the concepts within these theories allowed employees within the current study to feel prepared and act accordingly during the move to remote working. For example, data in the subtheme 'good and strong references to cyber-security culture' was indicative of beliefs that employees felt the security culture of the organisation was efficacious in producing good cyber-security behaviours. Therefore, the current research highlights how such theories might be applied to understand how organisations and employees coped behaviourally, whether positively or negatively, with the move to remote working during the pandemic and the perceptions of cyber security surrounding this area. This finding extends previous theoretical research, which has primarily looked at the impact of PMT, EPPM and ToPB concepts concerning preparedness for natural disasters such as flooding and earthquakes (Mulilis & Lippa, 1990; Tan et al., 2020; Tang & Feng, 2018; Weber et al., 2018). Future research should look at this in further detail to highlight the specific antecedents of the theory that might offer organisations direction as the current pandemic continues to see moves from office work to remote work and vice versa. Of course, the current research only finds participants to report feelings on preparedness rather than specific behaviours employees took to help them to prepare for the working from home scenario.

In wider research relating to PMT and risks, such as flood risk awareness and cyber-security, training on specific subjects or risks has been demonstrated to be one of the main justifications for preparedness at the collective level (Saban et al., 2021; Scolobig et al., 2012). Suggesting that the more people feel they are trained in certain situations, heightens their sense of preparedness. This links back to the idea surrounding the importance of

training employees in terms of cyber security and to the idea that the organisation was more prepared owing to the experience of needing to work from home previously urgently. Moreover, higher levels of trust are associated with positive evaluations of preparedness (Scolobig et al., 2012). It could be argued, therefore, that, given previous subthemes showing employee trust of the cyber-security team and wider security culture in Error! Reference source not found., such as 'it's managed for us', 'good and strong references to cyber-security culture' and 'separate but accessible; how infosec functions' within the organisation, this was one of the precursors to feeling prepared during COVID-19 and the move to remote working. Research within cyber security has demonstrated that as security awareness increases, so do feelings of preparedness for cyber security-related issues (Saban et al., 2021). This highlights that trust relating to cyber-security culture and cyber-security teams and feelings of security may help feelings of preparedness in risk situations beyond that of organisational cyber security, such as the move to remote working.

Arguably, the perceptions of preparedness put forward by participants could reflect attitudes of those who do not work within a cyber-security team; those receiving the benefits of cyber-security workers' labours and stress. The two information awareness professionals in the study argued that COVID-19 had made things slightly slower for them. The feelings of preparedness demonstrate that security teams can create an environment where employees feel safe and secure during this time, adding to the literature surrounding the impact of remote working on cyber security and how organisations are best placed to help employees.

7.6.2 Risk and Remote Working

Despite feelings of preparedness, participants in the current study highlighted some risks associated with working from home. The idea that people might be more relaxed at home and the proximity to which employees may work to others that they lived with was a discussion point among participants. This finding is similar to other pieces of surrounding literature where studies have shown that employees share remote working environments with unknown flatmates who may use this home-working period for malicious purposes (Nurse et al., 2021) or that employees may unintentionally share information with others.

The current research adds to this notion by presenting findings from a law firm, an industry where attorney-client privilege and the disclosure of confidential communications are of the utmost importance. It was pointed out that junior lawyers often share flats with other junior lawyers, often of different firms, which proposes a genuine issue in which, on purpose or not, confidential information could be shared. This puts the possibility of this risk, as discussed in Nurse et al. (2021) and Crossland and Ertan (2021), into a real context by demonstrating the reality of hypothesised remote working cyber-security issues.

Another risk considered in the wider research was that cyber-security awareness and training would be more challenging in a remote setting than in an office or that organisations would not be able to remotely train employees in cyber security effectively (Georgiadou et al., 2021, Nurse et al., 2021). This was not a prominent feature within the current research. From ongoing discussions with the organisation during this period and the write-up, it was clear that the organisation was able to give out sufficient training tailored to the remote environment context. However, in support of literature demonstrating an increase in cyber security attacks during the period of the pandemic (Chigada & Madzinga, 2021; Lallie et al., 2021; Muthuppalaniappan & Stevenson, 2021; Nurse et al., 2021), the two security professionals within the study did say there had been an increase in opportunistic phishing attacks against the organisation during this time. However, there was no data relevant to the progression of such attacks throughout the course of the pandemic.

Moreover, findings related to risk in cyber security gave credence to research showing that organisations and the workers within them generally cite human-related cyber-security issues as the biggest risk rather than technological issues (Goo et al., 2014; Hughes-Lartey et al., 2021; Lowry & Moody, 2015; Sabillon, 2022; Zimmerman & Renaud, 2019). This has been discussed in the previous findings' chapters, as were the consequences of this in relation to psychological theories such as PMT. However, it is perhaps worth highlighting again here that the human aspect was arguably seen as the weakest link in the remote working environment despite feelings of preparedness. This was the case despite many technological concerns that could arguably have been raised.

Furthermore, researchers have suggested that there has been a de-prioritisation of cyber security among workers because of heightened anxiety, stress, depression, and poor mental health caused by the pandemic (Nurse et al., 2021), with individuals needing to focus on their more basic, and vital, health needs. This is seen as a worry by some security professionals when it is coupled with the knowledge of the rise of cyber-security attacks during the pandemic. This arguably fits into a dialogue related to usable security. There is perhaps no question that it seems logical for employees of organisations, who have their own lives and worries, to focus on their more basic needs as a priority, especially during a global pandemic. Therefore, security professionals writing new security policies during this time need to consider their employees' priorities and not expect the impossible; for security to be a top concern. Future research should look at the degree to which this was considered and how security professionals should factor such concerns in when writing future policies.

7.6.3 Wellbeing

The participants in our study highlighted the sense of isolation from lack of face-to-face contact that they felt and how basic work tasks would become more challenging by not being in the same physical space as their colleagues. The impact on the mental health and wellbeing of employees has also been exemplified in broader work in this context (Khan et al., 2020; Lallie et al., 2020; Serafini et al., 2020; Xiao et al., 2021). For example, stressors related to home working have been linked to not having a separate workspace, care responsibilities for both children and sick friends/relatives, distractions from neighbours, poor Internet connection, technological issues related to the use of new work devices and the feeling of needing to be productive and efficient. This is in addition to broader stressors related to not being able to see family and friends. While not articulated directly by the participants in our study, the inability to have face-to-face contact with colleagues affected their work relations. The wider literature has also noted how repeated lockdowns, quarantine and work from home have led to higher workload, working more hours, anxiety caused by communicating less with co-workers, feelings of isolation, lower productivity, fatigue, and physical indicators such as bodily aches and pains (Khan et al., 2020; Lallie et al. 2020; Serafini et al., 2020; Xiao et al., 2021). Employees who were used to working in offices

have also been reported to suffer not only mental health but also physical health issues (Khan et al., 2020).

The emotional stressors of working from home and the uncertainty that surrounds the pandemic have also been linked to an increase in online threats. Emotions such as relief, fear and hope (Naidoo, 2020) have been argued to be the top three emotions that have been exploited during the COVID-19 pandemic. For example, there has been an increase in the number of phishing attacks experienced by employees during COVID-19, mentioned by participants in the current study and within wider research, which has been linked to a decrease in employees' general wellbeing (Georgescu, 2021). This is in addition to a rise in the ransomware attacks experienced by companies (Nurse et al., 2021), which has also been ascribed to the fact that employees have had to adapt to working from home routines, as phishing emails have been reported to have been the main reason for the increase in ransomware attacks (Georgescu, 2021). While the participants in our study spoke of organisational risks linked to them working from home, broader studies have noted how employees have been targeted explicitly through different online mediums, including video conferencing and online chat functions (Naidoo, 2020).

Moreover, the cyber-security architecture at home does not have the same levels of security as in organisations, with research arguing this to be even more the case if the home in question has been developed under a smart infrastructure scheme (Andrade et al., 2020). VPN solutions are used to protect telecommuting communications, but security attacks exploit vulnerabilities of home equipment and people so that VPN solutions could reduce their efficiency (Andrade et al., 2020). The increase in COVID-19-related spams and subsequent increase in cyber incidents suggest that the negative impact of the pandemic on the mental health and wellbeing of work from home employees was a significant factor that affected cyber-security behaviours during the COVID-19 (Williams et al., 2020).

7.6.4 Conclusions and Contributions

Overall, the discussion of these findings in relation to the surrounding HCI literature and psychological theory highlights where this research has supported, added to, or conflicted with previous work on the COVID-19 pandemic, cyber security and remote working. Firstly, the current research demonstrates that participants felt their organisation was prepared for the move to remote working and that they felt secure moving to a remote environment. This sentiment sat in contrast to findings and predictions in the surrounding literature (Crossland & Ertan, 2021; Georgiadou et al., 2021; Lallie et al., 2021; Nurse et al., 2021). It was demonstrated that PMT, EPPM and TPB models could be applied in the future to understand the antecedents to the degree of preparedness in organisations. These insights could help organisations understand how to develop future resilience. The remote risks noted in the surrounding literature (Nurse et al., 2021; Crossland & Ertan, 2021) were supported by participants from the case organisation and demonstrated the possibility of everyday security issues in remote working owing to living situations. Moreover, in the present findings, remote work security risks centred on `human risks' rather than technological ones, which fit into ideas in the surrounding literature that the 'human as the weakest link' is still the dominant thinking, despite research trying to promote positive security (Beautement & Sasse, 2009; Inglesant & Sasse, 2010; Nurse et al., Weirich & Sasse, 2001). Research and the findings of the current study further highlight that usable policies need to be considered within the context of the pandemic and the degree to which we can ask people to care about security, given the global context. Finally, the current study added to previous research on how repeated lockdowns, quarantine and work from home have led to issues related to wellbeing among employees (Khan et al., 2020; Serafini et al., 2020; Xiao et al., 2021; Zacher & Rudolph, 2021) which may heighten vulnerability to threats.

Chapter 8. Conclusion

8.1 Introduction

This thesis intended to understand cyber-security culture, behaviours and individual perceptions and biases within the context of a single organisation and the relationships between these dynamics. Secondly, this research investigates how the usable security and positive security narrative, along with psychological theories (PMT, the EPPM and the TPB), could be used to deepen these qualitative and contextual understandings. This was done through a case study of a global law firm, with 40 participants who partook in interviews or focus groups. Through the analysis of the data, four broad themes were produced. These were: external perceptions of cyber-security culture, the individual human element, perceptions of cyber-security training and policies, and the COVID-19 pandemic and the move to remote working. This thesis demonstrates the benefits of using established theories to understand cyber-security behaviours in a qualitative research context. This concluding chapter ties together key discussion points from the previous chapters while setting out the main contributions of this research. Such contributions are articulated with respect to theoretical, empirical, and methodological impact.

8.2 Summaries

8.2.1 Summary of Psychological Theories and Biases

As discussed in sections 2.2.2, 2.2.4 and 2.2.6 of Chapter 2, PMT, the EPPM and the TPB are influential models that attempt to understand and predict human behaviour. Many of the factors and concepts from the three psychological models appear in the current data. For example, as seen in PMT and the EPPM, notions of threat severity could be discovered when participants referenced the NotPetya cyber-attack in 2017. However, perceived threat vulnerability among the participants must also be considered. Many participants

demonstrated optimism when describing how likely the firm was to be a victim of a cyber-attack. This thesis, therefore, provides greater insight into perceived threat severity and how it might be combined with optimism to influence the overall perception of risk. This interaction is important to acknowledge when exploring cyber-security perceptions in the workplace, as both threat severity and optimism influence perceptions. Concepts within the coping appraisal of PMT, both self-and response-efficacy, known as efficacy beliefs in the EPPM, can also be seen in the findings. Participants believed their cyber-security culture to be 'good and strong'. However, they demonstrated consistent ideas that they, as the 'human factor' in the organisation, were and would always be the weakest link in cyber security. This could indicate that participants had low efficacy. Participants also displayed intrinsic and extrinsic benefits for purposely not performing protective actions against threats, i.e., timesaving.

Other displayed perceptions were linked to reduced protection motivation within the PMT model. For example, reduced responsibility could be a maladaptive thinking or defence strategy, whereby participants had diminished ideas of responsibility because they had low efficacy. PMT suggests that when employees perceive their organisations to be vulnerable to security threats, employees should become more motivated to protect their organisation. However, this assumes that employees also feel responsible for and able to conduct the required behaviours (Posey et al., 2014). If participants feel vulnerable to cyber-security threats and have low response efficacy, their motivation to respond will be low, and maladaptive thinking patterns may occur. Participants in the present study suggested that fee earners, in particular, take on less cyber-security responsibility and are less compliant with cyber-security policies than the business staff. Therefore, we observe that PMT sheds light on where participants' risk perceptions may lead to a reduction in behaving securely. In addition to presenting the applicability of PMT concepts to cyber security, this finding will assist in helping the case-study organisation and organisations more widely pinpoint where they can best improve security messaging, for example, by attempting to increase employee efficacy. Moreover, these findings highlight that organisations need to target individuals differently, as participant perceptions were not uniform.

In comparison to PMT, the EPPM suggests that fear leads to fear-control processes and that without fear or the combination of high efficacy and high perceived threat, an individual would have no response to a perceived threat. If fear did not occur in participants, the EPPM would argue that participants would not be motivated to act in response to any risk communications put out by the organisation. However, the EPPM's central concept of fear is perhaps not as evident in the current study, as most participants did not indicate having any overt fear perceptions towards cyber security. However, participants did demonstrate a level of behavioural compliance, and the fact they did not show an overt level of fear does not mean that fear did not exist. It is further possible that fear could have led to or been influenced by the optimism bias, as it has previously been demonstrated to have a moderating role on perceived threats (Chen et al., 2021). Moreover, it is conceivable that participants coped with a sense of fear by reducing their sense of responsibility, putting the main cyber-security responsibility on the cyber-security staff. It is probable that the EPPM is more suited to looking at direct responses to fear appeals rather than giving insight into individuals' perceptions and behaviour in a more naturalised and qualitative setting. The EPPM has further only been used a few times so far within the cyber-security domain and is perhaps more suited to health research, where risks are more personally clear.

Compared to the PMT and the EPPM, The TPB gives specific attention to social expectations or 'normative beliefs' and how perceived social pressure or subjective norms might influence behaviour. The impact of normative beliefs could be seen within participants' beliefs of culture, responsibility, such as 'it's managed for us', and compliance with policies. Participants understood it to be the norm that cyber security was managed elsewhere and that individuals, especially fee earners, might circumvent policies. This suggests mixed norms towards cyber security in the current organisation. Behavioural beliefs can be similarly understood in relation to individuals' perceptions of behaviour throughout the organisation, as well as probable outcomes of the possible behaviour and the assessments of these outcomes. For example, participants noted some recommended behavioural practices needed to be balanced with practical concerns, such as time taken. Finally, in this case, control beliefs, such as the human factor being the weakest link and optimistic beliefs that a cyber-security attack will 'not happen again' to the case-study organisation, were also visible in the current findings. In addition to presenting the applicability of TPB concepts to cyber

security in a case study and qualitative investigation, the findings will assist in helping the case-study organisation pinpoint where they can best improve security messaging. For example, by attempting to increase employee control beliefs and targeting organisational norms, or how the organisation might need to target individuals differently.

Different cognitive biases were found in the current data. The optimism bias, pessimistic views, and the availability heuristic were all present in the current findings. These biases were related to concepts within PMT and the EPPM. Firstly, the optimism bias was found to relate to beliefs surrounding the likelihood of future cyber-security events and perceptions that stemmed from the previous 2017 cyber-security attack on the organisation. Moreover, the current research showed a collective optimism bias, where individuals felt the firm, as a whole, was less at risk of falling victim to a cyber attack than other firms, rather than only themselves as individuals. Previous research has demonstrated that the optimism bias interferes with threat perceptions. Based on this, research has suggested that the optimism bias should be included in behavioural models, such as PMT and the EPPM, when the models are used to understand and predict cyber-security behaviours (Chen et al., 2021). For example, PMT suggests that people must perceive themselves as at risk from a certain threat if they are to undertake behaviours to deal with the threat.

Moreover, Chen et al. (2021) demonstrated that the optimism bias reduces risk perceptions and may lead to under-weighing of the assessed threats when developing intentions to cope with them. The present research arguably supports this idea by presenting that concept from these models and the optimism bias interacted in the current study. However, owing to the qualitative nature and focus of the current research, it is not possible to see exactly where these interactions might occur in the perception of risk process, and future research should aim to look at this. The availability heuristic, where people judge the likelihood of an event happening based on how easily they bring an example to mind (Harvey, 2007), was also found in the present findings. The availability heuristic was further considered as a possible explanation for the finding that human risks were the biggest cyber-security threats.

8.2.2 Summary of Usable Security Considerations

Throughout the findings chapters, we have seen how the results from the current study, add to and can be deepened by the usable security and wider HCI field. In Error! Reference source not found., usable security research demonstrated that the current findings corroborate and add to previous research on security culture by demonstrating beliefs of cultural differences between fee earning and support staff. The findings contribute to the debate of responsibility, by demonstrating that non-security participants and participants with cyber security or IT-related roles differ in opinion on how much responsibility staff should take for cyber security. Generally, participants outside IT and security-related roles believed staff should take less responsibility.

Chapter 5 emphasised some possible long-term benefits from experiencing a cyber-attack, such as improved awareness among participants. This corroborates research showing that post cyber-security attacks, participants understood the seriousness of such cyber-security policies and adhered to them better (e.g., Stacey et al., 2021). Previously, however, research has largely highlighted the negative impacts of a cyber-attack (e.g., Bada & Nurse, 2020; Czosseck et al., 2011; Genge et al., 2015; Gupta & Agarwal, 2017; Knight & Nurse, 2020). This suggests the possibility that the optimism bias was also present in participants' perceptions of the attack. Importantly, the 'human as a problem' mindset was seen throughout the findings, although arguably mainly present in Chapter 5. This finding aligns with previous usable security research, which has been attempting to change this 'human as the problem' dialogue for decades (e.g., Inglesant & Sasse, 2010; Kirlappos et al., 2013; Renaud, 2011; Sasse et al., 2001; Sasse & Rashid, 2021). The current research shows that the belief of the human as a weakness is not just exhibited by the security professionals in this organisation but also by individual non-security focussed employees. These findings highlight that if cyber security within organisations is to become better aligned with user-focussed 'positive security', it is essential to challenge dialogue framing humans as a weakness.

The findings from Chapter 6 lend support to previous studies that have demonstrated that employees may frequently report policy issues, such as authorisation operation issues

(Bartsch & Sasse, 2012), despite a high level of overall reported compliance. More broadly, the current findings support literature showing that employees are not always compliant (e.g., Blythe et al., 2015; Herath & Rao, 2009; Ifinedo, 2009; Siponen et al., 2010; Vance et al., 2012). However, the current research suggests that this is because of unusable aspects of security policy, as previously highlighted in usable security research (e.g., Beautement & Sasse, 2009; Inglesant & Sasse, 2010; Nurse et al., 2011a; Weirich & Sasse, 2001). PMT offered insight by demonstrating that when users perceive the benefits of non-compliant behaviours, this factors into their risk-perception process. User-experience research, the systematic research of users and their needs, has been a large part of technology development for decades (Glanznig, 2012). Such research is well documented, methodologies have been developed and honed, and user-centred design is now recognised to improve the user experience. Poor usability places demand on users, which impacts negatively on their productivity and, ultimately, that of the organisations in which they work by creating security problems of their own (Inglesant & Sasse, 2010; Kirlappos et al., 2013). Such research has not yet been widely applied to security policy within organisations. The current research also demonstrated specific pain points and individual thoughts on cyber-security training and awareness campaigns. This is useful not only by demonstrating where employees might be having difficulties but by indicating that asking employees for feedback is valuable. This again feeds into a wider dialogue of including the human in the cyber-security process and using employees as a resource for better security.

The findings showed that participants in the study appreciated the notion of phishing tests and found them useful. Previous research of a usable security nature has predicted and theorised that phishing one's own employees is likely to cause negative consequences and to be viewed negatively by employees (e.g. Kirlappos & Sasse, 2011; Kumaraguru et al., 2009; Kumaraguru et al., 2007; Sheng et al., 2010). The current research does not challenge this notion but argues that certain contextual factors, in this case, made such phishing campaigns a more positive experience for employees. It was found that in the current organisation, the phishing campaigns were conducted to be positive, whereby the firm reported the success of phishing attacks and did not use sanctions to discipline employees. In comparison to the current organisation, one previous study found the use of sanctions with regard to cyber-security behaviour campaigns, such as phishing simulations, to be found in 90% of the

organisations researched (Blythe et al., 2020). The psychological models offer further assistance in this context, as by making phishing campaigns positive, reporting the wins and not failures, the organisation would arguably be boosting the efficacy of employees by showing that they are capable and able to spot and report phishing emails. This study, therefore, presents a case where phishing tests have been used positively. Future research should look at providing guidance on how other industry professionals can accomplish this.

Finally, the current findings used both theoretical models and previous cyber-security research to inform the discussion of findings related to the COVID-19 pandemic in Chapter 7. Participants in the current study felt their organisation was prepared for the move to remote working, which contrasts with previous findings (e.g., Georgiadou et al., 2021; Lallie et al., 2021; Nurse et al., 2021). The PMT, EPPM and TPB models could be applied in the future to understand the antecedents to the degree of preparedness in organisations. The human risk was again the focus of any concerns related to remote working and cyber security, highlighting the human as the weakest link narrative again and suggesting consistency between beliefs during COVID-19 and more general beliefs. Furthermore, during the pandemic, as noted in the current study and other research (e.g. Beautement & Sasse, 2009; Inglesant & Sasse, 2010; Nurse et al., 2011a; Weirich & Sasse, 2001), individuals are experiencing increased levels of stress and anxiety. This highlights again the need for usable policies and questions the degree to which we can ask people to care about security, given the global context.

8.3 Theoretical Contributions

Broadly, the current findings contribute to theoretical understandings of PMT, the EPPM and the TPB, respectively, within the field of cyber security. The current research further fills a gap in the literature by exploring the perceptions and behaviours of employees within an organisation by employing both usable security and psychological theory together. These areas of research are often studied separately.

Previously, concepts within the aforementioned theories have been researched in isolation. Studies have conducted questionnaires and experiments to understand the correlations and relationships between intention and behaviour in cyber security. In such research, it is the relationships and influence of individual factors within theories are made experimentally clear, and these studies have been extremely impactful for the field (e.g., Blythe et al., 2015; Bulgurcu et al., 2010; Herath & Rao, 2009b; Ifinedo, 2009; Sommestad et al., 2015). However, such studies also remove the naturalised environment in which participants make these judgments due to their experimental nature. Hence, the current research aids and contributes to previous work by demonstrating the existence of theoretical concepts in a case study within a natural environment.

The current study further contributes to theory by demonstrating support for concepts within PMT, the EPPM, the TPB, and wider human factors of cyber security. As seen in PMT and the EPPM, concepts of efficacy and threat could be seen in the current findings. The TPB was discussed in terms of how behavioural beliefs, normative beliefs and control beliefs might be relevant to views of security culture. However, an overt finding of fear was not found in the study, perhaps because the current research does not study a specific cyber-security threat. Hence, the current research arguably offers less support to the EPPM. The EPPM has only been applied by researchers to cyber security within a few studies, the majority of which were published after the current research was completed (Chen et al., 2021; Masuch et al., 2021; Zhang & Borden., 2020). Therefore, the current research contributes theoretically by examining the application of the theory to the cyber-security field.

Based on the discovery of these concepts within this case study, the current research can hypothesise why individuals may not be holding correct beliefs about cyber-security issues or why they may be behaving in a certain manner. Using the lens of these theoretical theories further allowed the research to pinpoint how, within cognitive-behavioural models, perceptions of cyber security and behaviours in cyber security develop within the framework of organisational cyber security.

The current research studied cultural and individual cyber-security factors, along with cyber-security awareness and training, within the context of an organisation at a particular point in time. This provides researchers and professionals with information regarding user perceptions and behaviours, pinpointing where users struggle with aspects of certain policies and how these issues may combine to impact individuals' subsequent behaviour. With this deepened knowledge, researchers and industry professionals may be able to improve culture and policies for employees, which might, in turn, aid security.

The different findings related to the human element were found to be related to concepts in various psychological theories, PMT, the TPB and the EPPM. This is particularly important for the latter two theories, as they have not gained as much support in the area of cyber security. It was shown that the optimism bias could be both considered a maladaptive response to PMT constructs mechanism (Scheier & Carver, 1985) as well as a direct influence on individual threat appraisals (Chen et al., 2021). Thus, the current research extends PMT and EPPM research and lends possible support to the findings by Chen et al. (2021) by highlighting the optimism bias to influence risk concerns. Future research should aim to tease out these differences, perhaps in more controlled experiment-based studies.

Moreover, it was demonstrated that, through the lens of the theories, the perception of human aspects being the main risk to cyber security might reduce efficacy in individuals. This is important for future research and industry to consider, given the prominence of this view in research and wider media. It was demonstrated that PMT and TPB could offer insights into the consequences of policies having reduced security usability and aid understanding of how this might impact employees' cyber-security perceptions and behaviours.

It was suggested that PMT, EPPM and TPB models could be applied in the future to understand the antecedents to the degree of preparedness in organisations during the COVID-19 pandemic. This could help organisations understand how to develop future resilience. This further demonstrates how the current research suggests theoretical support for using psychological theory to research an emerging field, the understanding of cyber security within organisations during the COVID-19 pandemic.

8.4 Empirical Contributions

This thesis contributes to empirical research on usable security and research on the human factors of cyber security within organisations. Therefore, the current research both extends previous research and offers new insights into usable security issues.

The findings extended and added to cyber-security culture research in several ways. The data demonstrated that participants generally understood or saw the security culture of the organisation to be good and strong, relating to previous work on culture and how top management support in organisations is beneficial (Ashenden & Sasse, 2013; Hu et al., 2012; Uchendu et al., 2021). Participants also highlighted a few cultural differences. Participants saw a difference between the fee earning and support staff sides of the business regarding cyber-security behaviours. This extends previous work on cyber-security subcultures (e.g., Albrechtsen & Hovden, 2009; Da Veiga, 2016; Hofstede, 1998; Kolkowska, 2011; Muendo, 2014; Whelan, 2017) by demonstrating that cyber-security cultural differences may be found between fee earning and support staff in organisations. This finding also extends previous work from within law firms, where research has shown that the 'fee earner vs fee burner' mentality not only exists but may lead to low retention rates among support staff (Forstenlechner et al., 2009). There was also a perceived difference between law firms and other sectors, perhaps demonstrating a bias of participants to see their organisation as better. Previous research on responsibility suggests that the reduced cyber-security responsibility among fee earning staff could be why they are seen to behave less securely.

The current research contributed to our understanding of the optimism bias in cyber security. Findings relating to the optimism bias demonstrated the existence of a collective form of optimism that extends to the whole organisation. This is an important finding as, previously, optimism bias research in cyber security has been relatively individual (e.g., Campbell et al., 2007; Chmielarz & Szumski, 2019; Cho et al., 2010; Haltinner et al., 2015; Kim et al., 2018; Rhee et al., 2005; Rhee et al., 2012). The current research further demonstrated that the 2017 cyber-attack had a lasting impact on the firm. This finding compares to previous research by showing that the long-term repercussions of the attack were often

viewed positively rather than negatively. This may also have research implications for anyone specifically interested in NotPetya. Although, this finding could be a further example of the optimism bias. However, it is not clear what the repercussions of the optimism bias would be. For example, some research shows that the optimism bias leads individuals not to take protective action (Chmielarz & Szumski, 2019; Loske et al., 2013). However, other research shows it could also be beneficial for employees to be optimistic (Conversano et al., 2010). This highlights that there are a few ways to interpret the current findings and whether the optimism bias is positive or negative for cyber security.

Importantly, the current research adds to existing findings of the human as a weakness dialogue (Beautement et al., 2008; D'Arcy et al., 2014; Inglesant & Sasse, 2010; Renaud, 2011) as participants displayed consistent views that the human was the main point of weakness for cyber security and that employees believed themselves to be the weak link. Therefore, the extent to which participants could have efficacy if they believed themselves to be the weak link was questioned. This highlights that more work is needed in order for employees to be treated and feel as though they are part of solutions in cyber security. Importantly, this research demonstrates how psychological based and usable security-related research can complement each other to create a more coherent understanding of employees.

The current findings contribute to research on the perceptions of cyber-security training and policies. The findings demonstrated that the focus on human factors as threats in the current data supports previous work (Schaik et al., 2017; Zimmermann & Renaud, 2019). This idea is also a possible example of the availability heuristic (Tversky & Kahenman, 1974), perhaps one of the first empirical demonstrations of this heuristic in cyber security. The current research contributes to academic research and scholarship on phishing tests. Previous research has highlighted possible ethical and methodological issues with phishing one's employees. Despite this, the current research demonstrated that employees find phishing tests to be a useful exercise if done in a way that projects positivity.

Ideas concerning job roles suggested a split between ideas of responsibility between cyber security and IT professionals and other non-security roles. This was then related to the

concept of normative beliefs within the TPB. This again highlights differences between staff, which has implications for cyber-security awareness programmes and training. The findings related to behavioural practices and policy pain points were also related to the usable security literature (e.g., Beautement & Sasse, 2009; Inglesant & Sasse, 2010; Nurse et al., 2011a; Weirich & Sasse, 2001). It was demonstrated that future research should look at how cyber-security training might be best tailored to fit different cyber security needs and further demonstrated the usefulness of organisations creating feedback and dialogue with employees.

In contrast to existing research (e.g., Georgiadou et al., 2021; Lallie et al., 2021; Nurse et al., 2021), the current research demonstrated that they felt their organisation was prepared for the move to remote work. This finding contributes to existing work by suggesting how some employees were able to feel prepared for the move, owing to their previous experience of home working. This might be important for research as the world continues to work remotely and hybrid work. The remote risk noted in the surrounding literature (Nurse et al., 2021; Crossland & Ertan, 2021) were put into context, both in the pandemic and inside a law firm, demonstrating the possibility of everyday security issues in remote working owing to living situations. Previous research and the current study's findings further highlight that those usable policies need to be considered within the context of the pandemic and the degree to which we can ask people to care about security, given the global context. The current study further added to previous research on how repeated lockdowns, quarantine and work from home have led to issues related to wellbeing among employees (Khan et al., 2020; Serafini et al., 2020; Xiao et al., 2021; Zacher & Rudolph, 2021) which may heighten vulnerability to threats.

This research has drawn out several findings that will also be of interest to those working within the cyber-security industry, both in research and business. The identification of theoretical concepts will assist in helping the current organisation and future organisations pinpoint where they can best target cyber-security messaging and training, for example, by attempting to increase employee control beliefs and targeting organisational norms.

The research further demonstrates many instances where participants had different perceptions. Therefore, this shows the high degree to which organisations contain employees with different views and needs, meaning organisations need to target individuals differently. Participants also showed different wants and thoughts about security training and policies and gave specifics on issues and improvements. This emphasises that asking employees for feedback can be extremely valuable in cyber security. A notion that may seem simple but is often not taken advantage of (Reinfelder et al.,2019). The current research does note that not all organisations and industries may have the time or resources to do this; however, this approach might use fewer resources and money than implementing unusable policies that lead to non-compliant behaviours.

8.5 Methodological Contributions

This thesis studied the perceptions and behaviours of employees within an organisation via qualitative methods within a case study. This research method is relatively unique compared to the extensive quantitative and mixed methods research that dominates the cyber-security field. Therefore, the use of this method within this field advances the knowledge of this method and makes a methodological contribution to the field of cyber security by demonstrating its use in research and industry in this specific context.

Moreover, this method proved valuable in gaining impactful insights from participants. As research has stated, organisations need an improved feedback link between employees and information security policy and technology. This thesis achieved presenting an example of how this might be achieved. Of course, not all organisations will have access to this type of research or the time and money to complete research on this scale. However, this thesis demonstrates that conducting focus groups and interviews with employees do provide valuable insight.

More specifically, the current research demonstrated that discussing culture with participants can be a useful method, for research, rather than 'measuring' culture through instruments. The use of this method has implications for future research by presenting a new

employee inclusive technique for research. Moreover, the findings suggest that organisations should not only look at the impact of organisational cyber-security policies and their usability on employees but also how policies and cyber-security requirements in people's personal lives. For example, how many websites require different and complicated passwords. Moreover, future research and industry should aim to do more user experience research on their policies to improve them for employees and security.

8.6 Contributions to Industry and Practitioners

This research has drawn out several findings that will be of interest to those working within the cyber security industry, both in business and research. The identification of theoretical concepts will assist in helping the current organisation and future organisations pinpoint where they can best target cyber security messaging and training, for example by attempting to increase employee control beliefs, and targeting organisational norms. The current research also demonstrates how psychological based and usable security-related research can complement each other, to create a more coherent understanding of employees. Moreover, the current research has attempted to demonstrate how usable security can be used to empower employees rather than constrain them, which might be of importance to those developing cyber security strategy initiatives.

The research further demonstrates many instances where participants have different perceptions. Therefore, this shows the high degree to which organisations contain employees with different views and needs, meaning organisations need to target individuals differently. Participants also showed different wants and thoughts about security training and policies and gave specifics on issues and improvements. This emphasises that asking employees for feedback can be extremely valuable in cyber security. A notion that may seem simple, but that often is not taken advantage of (Reinfelder et al.,2019). This could be utilised by those wanting to create cyber security strategy initiatives tailored to individual organisations, and subgroups within organisations. The current research does note that not all organisations and industries may have the time or resources to do this, however, this

approach might use fewer resources and money than implementing unusable policies that lead to non-compliant behaviours.

The current research has implications for bridging research between academia and industry. There is not a wide degree of similar research at present within the cyber-security domain (Uchendu et al., 2021). Without such research, it would be challenging to ascertain the true value of previous theories and studies and whether they might impact the real-world cyber-security culture in situ. The current research hopefully, therefore, might provide an example for industry professionals where research has been successfully conducted and shared without the need for extensive NDAs and data sharing restrictions. The current organisation also expressed hope that this might be the case.

Finally, the present research has direct implications for the organisation in which this research took place. At the time of writing, the researcher is still in contact with the organisation and has presented the research to the cyber-security awareness specialists within the organisation. These individuals currently hope to take the current findings forward by presenting them to the board and using them as a basis to create future awareness and training programmes that better suit their employees.

8.7 Limitations and Future Directions

Despite the implications of the current research, it is notwithstanding limitations. Firstly, as discussed in the methodology, the current research is based on one case study, so its generalisability is limited. The current research does not argue that the results are generalisable, instead, it is argued that the research represents a base for future research and an example of how these methods can work in cyber security. In line with this limitation, even though the current organisation operates globally, all the current research was conducted with those from offices around the United Kingdom. Initially, the research had a more international outlook. However, owing to issues surrounding the pandemic, this did not prove viable. The generalisability of the current research should be extended by replicating the current findings in different contexts and countries. Moreover, a few high-level findings

also found in previous literature might be extrapolated. For example, the existence of cultural differences within one organisation were demonstrated in the current research and have been demonstrated previously (Da Veiga, 2016; Da Veiga & Martins, 2017; Hofstede, 1998; Kolkowska, 2011; Muendo, 2014; Whelan, 2017). It can therefore be expected that other organisations will contain some forms of cyber-security subcultures, even if these subcultures do not directly reflect those found previously.

Further, it is possible that there could be something specific about an organisation that willingly agrees to take part in research. Some might argue that the organisation has less to hide, or already has thought about and developed cyber-security practices when compared to other organisations. This is likely true, however, by promoting this type of research, we might hope to pave the way for different organisations participating in the research and therefore contributing to a more diverse research landscape.

As is generally the case when asking participants to report on their behaviour and perceptions, especially as security behaviours can be seen as being linked to job performance (Podsakoff et al., 2003), social desirability biases could have influenced participants' discussions. For example, participants may have underreported compliance issues or overreported the degree to which they felt the security culture was good. The researcher attempted to offset these issues by assuring the participants that everything they said would be anonymised and that the study was an attempt to learn from them rather than test them.

Moreover, as is the nature of the type of qualitative research conducted here, we can only provide support for the concepts of the theories discussed rather than the order in which these concepts occur. For example, it is not clear whether normative beliefs influence the intention to perform behaviours in the current research. However, these concepts and their process have been demonstrated in much research, both related to cyber security and outside of cyber security before.

The fact that the majority of the participants were 'fee burners' and not 'fee earners' may have also impacted the findings of the research in some way. Although the 'fee earners' in the current research did display similar perceptions and thinking around cyber security and

displayed views consistent with the 'fee burner's' interpretation of them. It is possible that we may have got more varying views if more 'fee burners' were included. However, due to the nature of this role, it is likely that most of the 'fee burners' in the current organisation did not have time to be interviewed, hence the low number of this demographic.

A few potential future directions have already been discussed throughout the last few sections of this chapter and the general discussion; however, these will be summarised here. Firstly, the current research suggests that future studies should aim to use participant discussion as a method to gain insight into cyber-security culture, perceptions, biases and behaviours. Future research might additionally look at whether the use of such methods helps employees within organisations feel included in the cyber-security process. In the current research, such findings were also deepened by using psychological theory and usable security together; future research might also benefit from using these two perspectives in combination.

It was also clear from the current research that future research could also explore various considerations of the optimism bias. For example, this study is one of the first to demonstrate a collective optimism bias. Future research should aim to investigate this in other organisations and scenarios to see if the phenomenon is widespread. The optimism bias was also found in conjunction with more pessimistic beliefs, suggesting the need to tease out when both of these occur and what it means if both occur simultaneously. Moreover, the influence of the optimism bias on risk perception theories should be further investigated to add to the current and Chen et al.'s (2021) research.

Researchers in cyber security, along with industry, need to further try and work with cyber-security experts to change the perception of the human as the problem in cyber security. The current research and many other studies show that employees and employers believe themselves, as humans, to be the weakest link in cyber security. Using the usable security literature together with PMT, the EPPM and the TPB, the current research has demonstrated why this concept of the self as the cyber-security problem might not be best for individuals, organisations, or security generally.

8.8 Lessons Learned: Tips for Future Researchers

In this section I will provide some lessons I learned from conducting this type of in-depth research with an organisation in the hope that it could aid other researchers in the field. However, it should be noted that this section is based purely on my personal experience during this research, and the experience of others is likely different.

Firstly, if you want to conduct research within an organisation, you need to find an organisation that will participate. This is probably the most difficult stage. As discussed in section 3.2.3, I approached this by emailing various contacts, provided by supervisors and myself. These were not just any random contacts within organisations, but contacts who worked specifically within cyber-security functions. This is important, as these people will likely have the biggest buy-in to your research, and control over whether the organisation participates. This is not to say you should not contact other people, dedicated programme managers or c-suite contacts would also be ideal. If you do not have any contacts, LinkedIn and Twitter can also be useful resources.

I ensured that the original email sent to organisations highlighted not only the proposed research and the benefits the research would provide to myself as a PhD student, but the benefits my research could provide to the organisation. Remember, you are an experienced researcher, offering to give in-depth insight into aspects of this organisation. This is an extremely valuable service, that organisations often pay competitive amounts for professionals to do. Of course, you may not have the business experience professionals have, and you are looking to provide research on a very specific topic, but you are also offering to do this for free.

Secondly, I was also lucky enough to find an organisation who did not require me to go through a strict NDA (non-disclosure agreement) process. If possible, I would recommend trying to do the same, this would enable you to share your research and therefore have

greater impact in the research field. Keep in mind that this stage can take a while, and plan accordingly.

Thirdly, when you have access to an organisation, you need to think about the appropriate research methods to use to investigate your topic. Throughout this thesis, I highlighted the benefits of online interviews and focus groups, and I do this these methods have their benefits. However, I used this method out of necessity during COVID-19 lockdowns. If I could go back and do my research again, I would do the interviews and focus groups in person. In person research will help you gain more context on the organisation you are doing the research with, you can experience the environment of your participants, and this might lend to a more in-depth ethnographic opportunity. It is also important you highlight to the organisation that participants will need to remain anonymous. You will send the organisation an anonymised final report, but they should never see any data that identifies an individual or group of individuals.

Fourthly, I will provide some very practical advice. When creating interview schedules, make sure you create diary invites for the participants. Before I started doing this half-way through my research, I had many no-shows. After I started sending diary invites, the no-shows lessened. Remember, although the organisation has agreed to the research, participants are just employees taking time out of their day to answer questions often quite abstract to them.

Finally, I would recommend meeting with your main contact/s in the organisation regularly during your research. This helps you build a strong relationship, and you can provide insights that may help them in some capacity along the way.

Chapter 9. Appendices

9.1 Appendix A: Topic Guides

9.1.1 Elite Interview Topic Guide

Topic 1: Job role

- Where do you sit in the organisation's structure?
- What role do you play in information security?
- Do you interact with the technological side of information security?

Topic 2: Security culture

- How do you view the security culture of the organisation?
    - As a whole
    - Differences and similarities between individuals/ offices/departments/countries
    - How do other people view it?
- What about cultural vision?
- How does this 'vision' translate into specific activities you do?

Topic 3: Resources

- How do you and your team secure resources?
- How do you talk to boards about needing resources?
- How do you decide what to spend resources on?

Topic 4: Information security measures/training

- What communications have you previously used / currently have in place?
- Why do you choose one method over the other?
- How to decide what to focus on?

Topic 5: data

- How do you use and keep data from campaigns and training you run, for example, phishing campaigns?

9.1.2 Focus Group Topic Guide

Welcome

- Introduction of research
- Information sheet, consent forms to be signed and demographics form to be completed
- Introduction of participants

Personal Threat

- How likely are you to be the victim of a cyber-attack? (open to interpretation, prompt if needed)
- Which threats do you feel impact you?
- Have WFH practices meant a change in your view on this?
- Why do you think some colleagues might be the victim of a cyber-attack?
- What are the consequences?
- Who is responsible?

Company threat

- How likely is the company to be the victim of a cyber-attack?
- Why?
- How likely are other law firms?
- Response efficacy of company policy
- Usability of company policies and software
- Experiences
- Did the company's previous data breach impact any views?

Opinions on behavioural interventions

- Ask if there are any people can think of
- Ask about accountability
- Ask about affirmation
- General training

Measures are given/taken to relieve the threat

- Self-efficacy
- Response cost

9.1.3 Interview Topic Guides

Topic guide for managers:

1. Behaviours

'I am going to ask you about your security behaviours'
'Your knowledge is as valuable as mine / you're the experts' – build up the Confidence'

Does security come into the way you see day to day activities in your job?

Does security come into the way you see and behave about your job?

- Daily
- Email
- Passwords
- Any other daily impact policies

2. Policy

What is your involvement in IS security policy?

- Do you inform policy?
- Would you like to?
- Would they see managers informing information security policy as important?

Have your company's current information security policies and strategies been accepted by employees well?

3. Culture

- Do people care about information security
- Does it differ between managers and employees?

How many people do you manage?

Do you see categorical differences in behaviours and attitudes between employees?

Do you act as someone who your employees go to manage?

Are employees seen as a weak link/solution?

I've been told your company employs a more human-centric and human as a solution focus to information security, have you found this to be true?

- What impact has this had?
- Do you think this has had a positive impact?

How are employees in terms of 'compliance'?

- Are managers better at complying?
- Do employees comply
- Are they receptive?

4. Resources

- Where do you and your employees go to seek information?
- Does the organisation provide adequate resources?
- Training?

Attitude speculation

How do employees view information security within the organisation?

- Do you believe they see cyber security as a top priority problem?
- Do employees understand and know about different threats?

Interaction

- Is there much interaction between employees and managers about cyber security?
- Do employees have or want to have input on policies?

Did the ransomware attack in 2017 have an impact on any of the company policies or your own behaviour?

Topic guide for employees:

1. Behaviours

'I am going to ask you about your own security behaviours'
'Your knowledge is as valuable as mine / you're the experts' – build up the Confidence'

Does security come into the way you see and behave in reference to your job?

- Daily
- Email
- Passwords
- Any other daily impact policies

2. Policy

What is your involvement in IS security policy?

- Do you inform policy?
- Would you like to?
- Would you see informing information security policy as important?

What do you think about the organisational policy?

- Anything that works well
- Anything that doesn't

3. Resources

- Where do you go to seek information?
- Does the organisation provide adequate resources?
- Training?

4. Campaigns

Do you like the current information security policies and campaigns? Do they work well?

- What impact has this had?
- Do you think this has had a positive impact?

5. Culture

Of the company in general

- Do people care about information security
- Why?
- Does it differ between managers and employees?
- Are people scared
- Or do they feel safe?

I've been told your company employs a more human-centric and human as a solution focus to information security, have you found this to be true?

Rewards and punishments

- Do they organisation reward or punish employees?
- Would you be responsive to either of?

6. Attitudes

Do you believe you and other employees are an asset/resource or maybe weakness?

Attitude speculation

- What do managers think about employees in terms of information security
- What do you think about managers?

Did the ransomware attack in 2017 have an impact on any of the company policies or your own behaviour, in your opinion?

9.2 Appendix B: Study Information Sheets

9.2.1 Elite Interviews

Participant Information form

Study Title: Perceptions in Information security

Invitation to take part
You are invited to take part in an interview as part of a Cyber Security PhD at Royal Holloway, University of London. Before you agree to take part, please read the following information carefully and ask the researchers if you have any questions or concerns.

Why is this research being done?
This study at your organisation forms part of a research project that will contribute to a three-year doctoral thesis on human factors in information security.

Who is doing the research?
I am a PhD researcher in the Information Security Group, Royal Holloway and I am co supervised in the Psychology Department. I am part of the Cyber Security Centre for Doctoral Training, which is sponsored by EPSRC grant EP/P009301/1.

What is the purpose of this study?

The purpose of this interview is to understand how your organisation and your role at this organisation is structured, how information security fits into the organisation, is viewed and rolled out, why decisions are made, and how employees are viewed and treated in terms of information security.

Do I have to take part?

No, it is your choice whether you participate or not and your participation is entirely voluntary. If you do decide to take part, then you are free to withdraw from the study at any time and you do not need to give a reason. During the focus group, you are also free to choose not to answer any questions or participate in certain discussions, without giving a reason.

What would taking part involve?

If you decide to take part, you will be asked to participate in a one to one discussion which will last around 40 minutes. You may be asked questions as a starting point for the discussion, but you may contribute anything you think is relevant to this discussion. Your real name or any identifying information will never be used in the write up of the report.

Will the discussion be recorded?

Yes, an audio recording of the discussion will be used to make a transcript for research purposes. You will be referred to via a pseudonym in the transcripts and any research report and publication, your real name or any identifying information will not be used.

Are there any disadvantages or risks to taking part?

You will not be disadvantaged in any way for taking part in this study. There are no substantial risks to taking part. However, if any of the questions make you feel uncomfortable, or you wish to find out more about cyber security threats, all participants will be provided with the contact information of the researcher and some useful informational websites.

Are there any benefits to taking part?

By taking part in this study you will provide valuable information that could help the researchers to gain new understanding of how cyber security behaviours and how threats are perceived. Ultimately this may help in the attempt to reduce cyber threats, by understanding where interventions are needed, or improving cyber security communications.

What will happen to the results?

As audio-recorded material will be transcribed at a later date, interview transcripts are likely to be stored in electronic format as an audiofile and a word-processed text file, for a period of time until December 2021 at the latest. The data will only be stored as long as necessary and will be permanently deleted as soon as the analysis and content has been finalised. Results will be written up for submission as part of my PhD thesis. It is also possible that the results of the project may be submitted for academic publications, blogs or presented to academic audiences. Results will be presented in terms of groups of individuals. If any individual data are presented or published, the data will be completely anonymous, without any means of identifying the individuals involved. The data will be held privately and will not be shared with unauthorised parties.

Will my information remain confidential?

All the information collected about you during the course of the research will be kept strictly confidential in accordance with current data protection regulations (for more information, please see Royal Holloway's Data Management Policy here). Data storage and access will also be managed in line with the General Data Protection Regulation Regulation (GDPR) (for more information on your rights when it comes to accessing interview-related data, please see Royal Holloway's Data Protection Policy here). You will not be able to be identified in any reports or publications. All data will be identified only by a code, with personal details kept in a locked file or secure computer with access only by the researcher. You will not be identified to the organisation; only anonymised reports will be fed back to the organisation.

Who can I contact about the study?

If you have any questions about the study, please contact us using the details below:

Researcher: Georgia.crossland.2013@live.rhul.ac.uk
Supervisors: m.cinnirella@rhul.ac.uk or rikke.jensen@rhul.ac.uk

9.2.2 Focus Groups

Participant Information form

Study Title: Perceptions in Information security

Invitation to take part

You are invited to take part in a focus group research study as part of a Cyber Security PhD at Royal Holloway, University of London. Before you agree to take part, please read the following information carefully and ask the researchers if you have any questions or concerns.

Why is this research being done?

This study at your organisation forms part of a research project that will contribute to a three-year doctoral thesis on human factors in information security.

Who is doing the research?

I am a PhD researcher in the Information Security Group, Royal Holloway and I am co supervised in the Psychology Department. I am part of the Cyber Security Centre for Doctoral Training, which is sponsored by EPSRC grant EP/P009301/1.

What is the purpose of this study?

The purpose of this study is to understand people's perceptions and behaviours in relation to information security threats, and what may impact or motivate these, with specific reference to the optimism bias. The study aims to understand how information security is perceived at your organisation. Furthermore, the study will look at where people receive information about cyber security threats. The study also aims to investigate the usefulness of information security information communications to change biases and will ask your opinion of some examples.

Do I have to take part?

No, it is your choice whether you participate or not and your participation is entirely voluntary. If you do decide to take part, then you are free to withdraw from the study at any time and you do not need to give a reason. During the focus group, you are also free to choose not to answer any questions or participate in certain discussions, without giving a reason.

What would taking part involve?

If you decide to take part, you will be asked to participate in a group discussion which will last around 40 minutes with 10-15 minutes to view and discuss some cyber security information extracts. You may be asked questions as a starting point for the discussion, but you may contribute anything you think is relevant to this discussion. Your real name or any identifying information will never be used in the write up of the report. The focus group discussion will consist of between 4 to 6 others.

Will the discussion be recorded?

Yes, an audio recording of the discussion will be used to make a transcript for research purposes. You will be referred to via a pseudonym in the transcripts and any research report and publication, your real name or any identifying information will not be used.

Are there any disadvantages or risks to taking part?

You will not be disadvantaged in any way for taking part in this study. There are no substantial risks to taking part. However, if any of the questions make you feel uncomfortable, or you wish to find out more about cyber security threats, all participants will be provided with the contact information of the researcher and some useful informational websites.

Are there any benefits to taking part?

By taking part in this study you will provide valuable information that could help the researchers to gain new understanding of how cyber security behaviours and how threats are perceived. Ultimately this may help in the attempt to reduce cyber threats, by understanding where interventions are needed, or improving cyber security communications.

What will happen to the results?

As audio-recorded material will be transcribed at a later date, interview transcripts are likely to be stored in electronic format as an audiofile and a word-processed text file, for a period of time until December 2021 at the latest. The data will only be stored as long as necessary and will be permanently deleted as soon as the analysis and content has been finalised. Results will be written up for submission as part of my PhD thesis. It is also possible that the results of the project may be submitted for academic publications, blogs or presented to academic audiences. Results will be presented in terms of groups of individuals. If any individual data are presented or published, the data will be completely anonymous, without any means of identifying the individuals involved. The data will be held privately and will not be shared with unauthorised parties.

Will my information remain confidential?

All the information collected about you during the course of the research will be kept strictly confidential in accordance with current data protection regulations (for more information, please see Royal Holloway's Data Management Policy here). Data storage and access will also be managed in line with the General Data Protection Regulation Regulation (GDPR) (for more information on your rights when it comes to accessing interview-related data, please see Royal Holloway's Data Protection Policy here). You will not be able to be identified in any reports or publications. All data will be identified only by a code, with personal details kept in a locked file or secure computer with access only by the researcher. You will not be identified to the organisation; only anonymised reports will be fed back to the organisation.

Who can I contact about the study?

If you have any questions about the study, please contact us using the details below:

Researcher: Georgia.crossland.2013@live.rhul.ac.uk
Supervisors: m.cinnirella@rhul.ac.uk or rikke.jensen@rhul.ac.uk

9.2.3 Interviews

Participant Information form

Study Title: Perceptions in Information security

Invitation to take part

You are invited to take part in an interview research study as part of a Cyber Security PhD at Royal Holloway, University of London. Before you agree to take part, please read the following information carefully and ask the researchers if you have any questions or concerns.

Why is this research being done?

This study at your organisation forms part of a research project that will contribute to a three-year doctoral thesis on human factors in information security.

Who is doing the research?

I am a PhD researcher in the Information Security Group, Royal Holloway and I am co supervised in the Psychology Department. I am part of the Cyber Security Centre for Doctoral Training, which is sponsored by EPSRC grant EP/P009301/1.

What is the purpose of this study?

The purpose of this study is to understand people's perceptions and behaviours in relation to information security threats, and how they view other employees' attitudes and behaviours. The study aims to understand how information security is perceived at your organisation.

Do I have to take part?

No, it is your choice whether you participate or not and your participation is entirely voluntary. If you do decide to take part, then you are free to withdraw from the study at any time and you do not need to give a reason. During the interview, you are also free to choose not to answer any questions or participate in certain discussions, without giving a reason.

What would taking part involve?

If you decide to take part, you will be asked to participate in an interview which will last around 30-45 minutes. You may be asked questions as a starting point for the discussion, but you may contribute anything you think is relevant to this discussion. Your real name or any identifying information will never be used in the write up of the report.

Will the discussion be recorded?

Yes, an audio recording of the discussion will be used to make a transcript for research purposes. You will be referred to via a pseudonym in the transcripts and any research report and publication, your real name or any identifying information will not be used.

Are there any disadvantages or risks to taking part?

You will not be disadvantaged in any way for taking part in this study. There are no substantial risks to taking part. However, if any of the questions make you feel uncomfortable, or you wish to find out

more about cyber security threats, all participants will be provided with the contact information of the researcher and some useful informational websites.

Are there any benefits to taking part?

By taking part in this study you will provide valuable information that could help the researchers to gain new understanding of how cyber security behaviours and how threats are perceived. Ultimately this may help in the attempt to reduce cyber threats, by understanding where interventions are needed, or improving cyber security communications.

What will happen to the results?

As audio-recorded material will be transcribed at a later date, interview transcripts are likely to be stored in electronic format as an audiofile and a word-processed text file, for a period of time until December 2021 at the latest. The data will only be stored as long as necessary and will be permanently deleted as soon as the analysis and content has been finalised. Results will be written up for submission as part of my PhD thesis. It is also possible that the results of the project may be submitted for academic publications, blogs or presented to academic audiences. Results will be presented in terms of groups of individuals. If any individual data are presented or published, the data will be completely anonymous, without any means of identifying the individuals involved. The data will be held privately and will not be shared with unauthorised parties.

Will my information remain confidential?

All the information collected about you during the course of the research will be kept strictly confidential in accordance with current data protection regulations (for more information, please see Royal Holloway's Data Management Policy here). Data storage and access will also be managed in line with the General Data Protection Regulation Regulation (GDPR) (for more information on your rights when it comes to accessing interview-related data, please see Royal Holloway's Data Protection Policy here). You will not be able to be identified in any reports or publications. All data will be identified only by a code, with personal details kept in a locked file or secure computer with access only by the researcher. You will not be identified to the organisation; only anonymised reports will be fed back to the organisation.

Who can I contact about the study?

If you have any questions about the study, please contact us using the details below:

Researcher: Georgia.crossland.2013@live.rhul.ac.uk
Supervisors: m.cinnirella@rhul.ac.uk or rikke.jensen@rhul.ac.uk

9.3 Appendix C: Consent form

Participant Consent Form
Study Title: Perceptions in Information security

Having read the information sheet, please answer the following questions:-

I confirm that I have read and understood the information sheet and had any questions I asked answered to my satisfaction

YES NO (please delete one)

I confirm that I understand that I may leave the focus group/Interview at any time and refuse to answer any question, without giving a reason

YES NO (please delete one)

I confirm that I agree to take part in this focus group study

YES NO (please delete one)

I confirm that I am happy to have the focus group discussion recorded

YES NO (please delete one)

I confirm that I understand that these recordings will be kept anonymous by the researcher

YES NO (please delete one)

Name: _____ (please print)

Signature _____ Date _____

9.4 Appendix D: Demographic Questions

Participant Demographics form
Study Title: Perceptions in Information security

Having read the information sheet and having signed the consent form, please answer the following demographic questions:
Note: these questions will be used to gage the range of participants involved in the study and will not be used to later identify participants.

1 - Please indicate your gender (please circle one)

Female Male Other Prefer not to say

2 - Please state your age

_____

3 – What is your Nationality?

_____

4 – Please state your job title

_____

5 – Please tell us which department you work in

_____

9.5 Appendix E: Debrief

Participant Debrief Sheet

Study Title: Perceptions in Information security

Thank you for taking part in this focus group/Interviw
ew research study, which was carried out as part of a Cyber Security PhD at Royal Holloway, University of London. The purpose of this study was to gain a greater understanding of the optimism bias in relation to information security threats in your workplace. We also looked at what may impact or motivate these perceptions and behaviours. Furthermore, the study looked at where people receive information about cyber security threats. The study also aims to investigate the usefulness of information security communications, and whether such communications are considered to be persuasive in influencing the optimism bias, and how they might be improved.

If you want to find out more information about cyber security threats, and how such threats can be reduced, the UK National Cyber Security Centre (https://www.ncsc.gov.uk) provide information and guidance on this, both in relation to businesses and the home. Or talk to the relevant people at your workplace.

Furthermore, if you have been the victim of cyber-crime, and a discussion about this has made you feel upset, you can get support and find out more from Victim Support's cyber-crime page https://www.victimsupport.org.uk/crime-info/types-crime/cyber-crime.

Who can I contact about the study?

If you have any questions about the study, please contact us using the details below:

Researcher: Georgia.crossland.2013@live.rhul.ac.uk
Supervisor: m.cinnirella@rhul.ac.uk

9.6 Appendix F: Vignettes

9.6.1 Vignette 1

'I never believed that I would be a victim of a cyber-attack. I thought I was of little interest to 'hackers'. I also thought I would be able to spot a phishing email if I was sent one, I thought phishing emails would be of poor quality, with spelling mistakes and poor-quality logos. I was wrong. I received an email from what looked like my bank, telling me that my account had been compromised and asking for an update of various pieces of personal information such as my username, password and some bank account details. A few days later I lost all the money on my debit card. This has made me realise, everyone is the intended target of these attacks, and I need to be more careful. I know now that I should keep my security software up to date and that banks will not ask me to click on an email link.'

9.6.2 Vignette 2

Information-security threats (also called cyber security threats), such as phishing, computer viruses and malware are on the rise. A recent study demonstrates that 80% of people are unable to consistently identify phishing emails. Cyber criminals use phishing emails to encourage individuals (victims) to click on links to websites they've created solely for the purpose of information theft. They trick users into typing their names, addresses, login IDs, passwords, and/or credit card information into fields on sites that look like they belong to real companies. In some cases, just clicking the link provided in the email could automatically download malware onto the user's device. Once the malware is installed, hackers can easily steal the victim's information without their knowledge.
To better protect yourself from becoming a victim of a phishing scam, a security expert offers the following advice:

- Keep your security software and browsers up to date
- Hover over links to identify obvious fakes; make sure that an embedded link is taking you to the exact website it purports to be
- Take your time and inspect emails for obvious red flags: misspelled words, incorrect URL domains, unprofessional and suspicious visuals and unrecognized senders
- Instead of clicking on a link provided in an email, visit the website of the company that allegedly sent the email and log in to provide information this way.

9.6.3 Vignette 3

This quote is from 'Jamie' who works at a law firm.

'I have recently been the victim of a phishing attack. I had my bank account accessed and money stolen because I clicked on a link, thinking it was my bank, and filled out the information asked of me. This included some bank details as well as some personal information such as my date of birth, username and password. This has made me realise, everyone is the intended target of these attacks, and I need to be more careful. To prevent

further instances like this, we all need to keep security software up to date and be cautious when clicking on email links.'

9.7 Appendix G: Code Book

9.7.1 Individual Human Element Nodes

Name	Files	Referen...
The human element (I)	20	126
Mention of Cyber Attack	20	68
Human as hinderance	18	24
Biases	14	29
Optimism Bias	11	25
negative views	3	3
The human element (FG)	7	129
Mention of cyber attack	7	43
Human barrier and imp...	4	11
Biases	7	75
Pessimistic	6	13
personal and organi...	1	1
Personal	6	16
other factors	6	14
Optimistic	7	31

9.7.2 Perceptions of Cyber Security Training and Policies Nodes

The organisation and poli...	21	256
Usability	16	24
Training	20	76
Should be less easy	1	1
Risks or Threats	12	38
Reinforcers	4	6
Practices	14	42
Job Role	19	46
compliance	2	3
Awareness	2	3
The organisation and poli...	7	168
Threat examples	7	25
Protective steps	2	11
Organisational Policies	7	25
Job role	7	22
Awareness and training	7	85

9.7.3 The COVID-19 Pandemic and Remote Working Nodes

RW and the Pandemic (FG)	7	45
smooth transition	7	21
prepared	1	1
No change	5	15
cyber attach	1	1
negatives	7	17
miss face to face	2	2
increased risk	5	11
improved risk	2	2
feel secure and suppor...	3	3
Awareness and training	2	2
RW and Pandemic (I)	19	57
Well prepared	7	8
No impact	5	6
Miss social aspects	3	4
Feel supported	5	5
Changed cyber security	12	20

9.7.4 Security Culture Nodes

Security Culture (I)	14	24
Views of infosec	17	41
Infosec are IT	6	11
Give feedbackwork...	10	18
feeling Safe	4	4
A hinderance	1	2
responsibility	12	44
Trusting others	1	2
supervison	1	1
Managed for us	10	29
Individual responsibi...	4	7
Combination	4	4
Cultural differences	19	83
Lawyers fee earner...	10	23
Law sector increase...	11	29
Hierachical split	7	13
Department split	2	2
age	1	2
Security Culture (FG)	14	41
Responsibility	5	12
Positive	1	3
Help seeking behaviours	5	8
Feeling safe	2	5
Caring attitudes security	7	13

References

Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behaviour & Information Technology*, *33*(3), 237-248. https://doi.org/10.1080/0144929X.2012.708787

Acar, Y., Fahl, S., & Mazurek, M. L. (2016, November). You are not your developer, either: A research agenda for usable security and privacy research beyond end users. In *2016 IEEE Cybersecurity Development (SecDev)* (pp. 3-8). IEEE. https://doi.org/10.1109/secdev.2016.013

Adams, A., & Sasse, M. A. (1999). Users are not the enemy. *Communications of the ACM*, *42*(12), 40-46. https://dl.acm.org/doi/10.1145/322796.322806

Agrafiotis, I., Nurse, J. R., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity*, *4*(1), tyy006. https://doi.org/10.1093/cybsec/tyy006

Ahmad, T. (2020). Corona virus (covid-19) pandemic and work from home: Challenges of cybercrimes and cybersecurity. *Available at SSRN 3568830*. http://dx.doi.org/10.2139/ssrn.3568830

Ajzen, I. (1985). From intentions to actions: A theory of planned behavior. In *Action control* (pp. 11-39). Springer, Berlin, Heidelberg. https://link.springer.com/chapter/10.1007/978-3-642-69746-3_2

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, *50*(2), 179-211. https://doi.org/10.1016/0749-5978(91)90020-T

Ajzen, I. (2002). Perceived behavioral control, self-efficacy, locus of control, and the theory of planned behavior 1. *Journal of Applied Social Psychology*, *32*(4), 665-683. https://doi.org/10.1111/j.1559-1816.2002.tb00236.x

Ajzen, I., & Driver, B. L. (1992). Application of the theory of planned behavior to leisure choice. *Journal of Leisure Research*, *24*(3), 207-224. https://doi.org/10.1080/00222216.1992.11969889

Albrecht, M. R., Blasco, J., Jensen, R. B., & Mareková, L. (2021). Collective Information Security in Large-Scale Urban Protests: the Case of Hong Kong. *arXiv preprint arXiv:2105.14869*. https://www.usenix.org/conference/usenixsecurity21/presentation/albrecht

Albrechtsen, E., & Hovden, J. (2009). The information security digital divide between information security managers and users. *Computers & Security*, *28*(6), 476-490. https://doi.org/10.1016/j.cose.2009.01.003

Albladi, S. M., & Weir, G. R. (2020). Predicting individuals' vulnerability to social engineering in social networks. *Cybersecurity*, *3*(1), 1-19. https://doi.org/10.1186/s42400-020-00047-5

Aldasoro, I., Frost, J., Gambacorta, L., & Whyte, D. (2021). *Covid-19 and cyber risk in the financial sector* (No. 37). Bank for International Settlements. https://ideas.repec.org/p/bis/bisblt/37.html

Ali, O., Shrestha, A., Chatfield, A., & Murray, P. (2020). Assessing information security risks in the cloud: A case study of Australian local government authorities. *Government Information Quarterly*, *37*(1), 101419. https://doi.org/10.1016/j.giq.2019.101419

Alsaawi, A. (2014). A critical review of qualitative interviews. *European Journal of Business and Social Sciences*, *3*(4), 149-156. http://dx.doi.org/10.2139/ssrn.2819536

Alwan, H. B. (2018). Policy Development and Frameworks for Cyber Security in Corporates and Law Firms. *International Journal of Legal Information*, *46*(3), 137-162. https://doi.org/10.1017/jli.2018.41

Andrade, R. O., Ortiz-Garcés, I., & Cazares, M. (2020, July). Cybersecurity attacks on Smart Home during Covid-19 pandemic. In *2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4)* (pp. 398-404). IEEE. https://doi.org/10.1109/worlds450073.2020.9210363

Antunes, M., Maximiano, M., Gomes, R., & Pinto, D. (2021). Information Security and Cybersecurity Management: A Case Study with SMEs in Portugal. *Journal of Cybersecurity and Privacy*, *1*(2), 219-238. https://doi.org/10.3390/jcp1020012

Archibald, M. M., Ambagtsheer, R. C., Casey, M. G., & Lawless, M. (2019). Using zoom videoconferencing for qualitative data collection: perceptions and experiences of researchers and participants. *International Journal of Qualitative Methods*, *18*, 1-8. https://doi.org/10.1177/1609406919874596

Ashenden, D. (2018). In their own words: employee attitudes towards information security. *Information & Computer Security*, *26*(3), 327 337. https://doi.org/10.1108/ICS-04-2018-0042

Ashenden, D. M., Coles-Kemp, L., & O'Hara, K. (2018). Why Should I? Cybersecurity, the Security of the State and the Insecurity of the Citizen. *Politics and Governance*, *6*(2), 41-48. https://doi.org/10.17645/pag.v6i2.1333

Ashenden, D., & Sasse, A. (2013). CISOs and organisational culture: Their own worst enemy?. *Computers & Security*, *39*, 396-405. https://doi.org/10.1016/j.cose.2013.09.004

Bada, M., & Nurse, J. R. (2020). The social and psychological impact of cyberattacks. In *Emerging cyber threats and cognitive vulnerabilities* (pp. 73-92). Academic Press. https://doi.org/10.1016/B978-0-12-816203-3.00004-6

Bada, M., & Nurse, J. R. (2019). Developing cybersecurity education and awareness programmes for small-and medium-sized enterprises (SMEs). *Information & Computer Security*, *27*(3), 393-410. https://doi.org/10.1108/ICS-07-2018-0080

Bada, M., Sasse, A. M., & Nurse, J. R. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour?. *arXiv preprint arXiv:1901.02672*. https://doi.org/10.48550/arXiv.1901.02672

Baek, Y. M., Kim, E. M., & Bae, Y. (2014). My privacy is okay, but theirs is endangered: Why comparative optimism matters in online privacy concerns. *Computers in Human Behavior*, *31*, 48-56. https://doi.org/10.1016/j.chb.2013.10.010

Baig, K., Kazan, E., Hundlani, K., Maqsood, S., & Chiasson, S. (2021). Replication: Effects of Media on the Mental Models of Technical Users. In *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)* (pp. 119-138). https://www.usenix.org/system/files/soups2021-baig.pdf

Balozian, P., Leidner, D., & Warkentin, M. (2019). Managers' and employees' differing responses to security approaches. *Journal of Computer Information Systems, 59*(3), 197-210. https://doi.org/10.1080/08874417.2017.1318687

Barnett, D. J., Balicer, R. D., Thompson, C. B., Storey, J. D., Omer, S. B., Semon, N. L., ... & Norbin, J. A. (2009). Assessment of local public health workers' willingness to respond to pandemic influenza through application of the extended parallel process model. *PloS one*, *4*(7), e6365. https://doi.org/10.1371/journal.pone.0006365

Barnett, J., & Breakwell, G. M. (2001). Risk perception and experience: Hazard personality profiles and individual differences. *Risk Analysis*, *21*(1), 171-178. https://doi.org/10.1111/0272-4332.211099

Barnett, J., & Breakwell, G. M. (2003). The social amplification of risk and the hazard sequence: The October 1995 oral contraceptive pill scare. *Health, Risk & Society*, *5*(3), 301-313. https://doi.org/10.1080/1369857031000160699 6

Barriball, L. K., & While, A. (1994). Collecting Data using a semi-structured interview: a discussion paper. *Journal of Advanced Nursing*, *19*(2), 328-335. https://www.academia.edu/download/46633185/Collecting_data_using_a_semi-structured_20160619-3750-1na3fr8.pdf

Barron, A. (1998). Designing Web-based training. *British Journal of Educational Technology*, *29*(4), 355-370. https://doi.org/10.1111/1467-8535.00081

Bartsch, S., & Sasse, M. A. (2012). How users bypass access control and why: the impact of authorization problems on individuals and the organization. https://discovery.ucl.ac.uk/id/eprint/1389948/

Bauer, S., Bernroider, E. W., & Chudzikowski, K. (2017). Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks. *Computers & Security*, *68*, 145-159. https://doi.org/10.1016/j.cose.2017.04.009

Bayl-Smith, P., Taib, R., Yu, K., & Wiggins, M. (2021). Response to a phishing attack: persuasion and protection motivation in an organizational context. *Information & Computer Security*, *30*(1), 63-78. https://doi.org/10.1108/ICS-02-2021-0021

Beautement, A., & Sasse, A. (2009). The economics of user effort in information security. *Computer Fraud & Security*, *29*(10), 8-12. https://doi.org/10.1016/S1361-3723(09)70127-7

Beautement, A., Sasse, M. A., & Wonham, M. (2008, September). The compliance budget: managing security behaviour in organisations. In *Proceedings of the 2008 New Security Paradigms Workshop* (pp. 47-58). https://doi.org/10.1145/1595676.1595684

Becker, I., Parkin, S., & Sasse, M. A. (2017). Finding security champions in blends of organisational culture. *Proc. USEC*, *11*. http://dx.doi.org/10.14722/eurousec.2017.23007

Befort, C. A., Nazir, N., Engelman, K., & Choi, W. (2013). Fatalistic cancer beliefs and information sources among rural and urban adults in the USA. *Journal of Cancer Education*, *28*(3), 521-526. https://doi.org/10.1007/s13187-013-0496-7

Bellmann, L., & Hübler, O. (2020). Working from home, job satisfaction and work–life balance–robust or heterogeneous links?. *International Journal of Manpower*, *42*(3), 424-441. https://doi.org/10.1108/ijm-10-2019-0458

Benenson, Z., Lenzini, G., Oliveira, D., Parkin, S., & Uebelacker, S. (2015, September). Maybe poor johnny really cannot encrypt: The case for a complexity theory for usable security. In *Proceedings of the 2015 New Security Paradigms Workshop* (pp. 85-99). https://doi.org/10.1145/2841113.2841120

Beris, O., Beautement, A., & Sasse, M. A. (2015, September). Employee rule breakers, excuse makers and security champions: Mapping the risk perceptions and emotions that drive security behaviors. In *Proceedings of the 2015 New Security Paradigms Workshop* (pp. 73-84). https://doi.org/10.1145/2841113.2841119

Bhattacherjee, A., & Shrivastava, U. (2018). The effects of ICT use and ICT Laws on corruption: A general deterrence theory perspective. *Government Information Quarterly*, *35*(4), 703-712. https://doi.org/10.1016/j.giq.2018.07.006

Berry, D. (2004). *Risk, communication and health psychology*. McGraw-Hill Education (UK). https://doi.org/10.7748/phc.14.7.10.s15

Birmingham, W. C., Hung, M., Boonyasiriwat, W., Kohlmann, W., Walters, S. T., Burt, R. W., ... & Hill, D. A. (2015). Effectiveness of the extended parallel process model in promoting colorectal cancer screening. *Psycho-Oncology*, *24*(10), 1265-1278. https://doi.org/10.1002/pon.3899

Blaine, B., & Crocker, J. (1993). Self-Esteem and Self-Serving Biases in Reactions to Positive and Negative Events: An Integrative Review. *Self-Esteem*, 55–85. https://doi.org/10.1007/978-1-4684-8956-9_4

Blanton, H., Gerrard, M., & McClive-Reed, K. P. (2013). Threading the needle in health-risk communication: Increasing vulnerability salience while promoting self-worth. *Journal of Health Communication*, *18*(11), 1279-1292. https://doi.org/10.1080/10810730.2013.778359

Bloom, N., Liang, J., Roberts, J., & Ying, Z. J. (2015). Does working from home work? Evidence from a Chinese experiment. *The Quarterly Journal of Economics, 130*(1), 165-218. https://doi.org/10.1093/qje/qju032

Blower, S. M., & McLean, A. R. (1994). Prophylactic vaccines, risk behavior change, and the probability of eradicating HIV in San Francisco. *Science*, *265*(5177), 1451-1454. https://doi.org/10.1126/science.8073289

Blum, D. (2020). Strengthen security culture through communications and awareness programs. In *Rational Cybersecurity for Business* (pp. 91-122). Apress, Berkeley, CA. https://doi.org/10.1007/978-1-4842-5952-8_4

Blumenthal-Barby, J. S., & Krieger, H. (2015). Cognitive biases and heuristics in medical decision making: a critical review using a systematic search strategy. *Medical Decision Making*, *35*(4), 539-557. https://doi.org/10.1177/0272989x14547740

Blythe, J., & Camp, L. J. (2012, May). Implementing mental models. In *2012 IEEE Symposium on Security and Privacy Workshops* (pp. 86-90). IEEE. https://doi.org/10.1109/spw.2012.31

Blythe, J. M., Coventry, L., & Little, L. (2015). Unpacking security policy compliance: The motivators and barriers of employees' security behaviors. In *Eleventh Symposium On*

Usable Privacy and Security ({SOUPS} 2015) (pp. 103-122). https://doi.org/10.1145/1572532.1572595

Blythe, J. M., Gray, A., & Collins, E. (2020, July). Human Cyber Risk Management by Security Awareness Professionals: Carrots or Sticks to Drive Behaviour Change?. In *International Conference on Human-Computer Interaction* (pp. 76-91). Springer, Cham. https://doi.org/10.1007/978-3-030-50309-3_6

Bødker, S. (2015). Third-wave HCI, 10 years later---participation and sharing. *Interactions*, *22*(5), 24-31. https://doi.org/10.1145/2804405

Bødker, S. (2006, October). When second wave HCI meets third wave challenges. In *Proceedings of the 4th Nordic conference on Human-computer interaction: changing roles* (pp. 1-8). https://doi.org/10.1145/1182475.1182476

Bokhove, C., & Downey, C. (2018). Automated generation of 'good enough' transcripts as a first step to transcription of audio-recorded data. *Methodological Innovations*, *11*(2), 2059799118790743. https://doi.org/10.1177/2059799118790743

Boss, S., Galletta, D., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly*, *39*(4), 837–864. https://doi.org/10.25300/misq/2015/39.4.5

Bowen, S. A. (2002). Elite executives in issues management: The role of ethical paradigms in decision making. *Journal of Public Affairs, 2*(4), 270-283. https://doi.org/10.1002/pa.119

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77-101. https://doi.org/10.1191/1478088706qp063oa

Braun, V., & Clarke, V. (2021). To saturate or not to saturate? Questioning data saturation as a useful concept for thematic analysis and sample-size rationales. *Qualitative Research in Sport, Exercise and Health*, *13*(2), 201-216. https://doi.org/10.1080/2159676x.2019.1704846

Breakwell, G. M. (2014). *The psychology of risk*. Cambridge University Press. https://doi.org/10.1177/0959354310210010902

Briggs, P., Jeske, D., & Coventry, L. (2017). Behavior change interventions for cybersecurity. In *Behavior change research and theory* (pp. 115-136). Academic Press. https://doi.org/10.1016/b978-0-12-802690-8.00004-9

Brostoff, S., & Sasse, M. A. (2003). "Ten strikes and you're out": Increasing the number of login attempts can improve password usability. https://discovery.ucl.ac.uk/id/eprint/19826/

Brown, W. J., & Basil, M. D. (1995). Media celebrities and public health: Responses to 'Magic' Johnson's HIV disclosure and its impact on AIDS risk and high-risk behaviors. *Health Communication*, *7*(4), 345-370. https://doi.org/10.1207/s15327027hc0704_4

Brown, J. P., Martin, D., Nagaria, Z., Verceles, A. C., Jobe, S. L., & Wickwire, E. M. (2020). Mental health consequences of shift work: an updated review. *Current Psychiatry Reports*, *22*(2), 1-7. https://doi.org/10.1007/s11920-020-1131-z

Budimir, S., Fontaine, J. R., & Roesch, E. B. (2021). Emotional experiences of cybersecurity breach victims. *Cyberpsychology, Behavior, and Social Networking*, *24*(9), 612-616. https://doi.org/10.1089/cyber.2020.0525

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, *34*(3), 523-548. https://doi.org/10.2307/25750690

Burdon, M., & Coles-Kemp, L. (2019). The significance of securing as a critical component of information security: An Australian narrative. *Computers & Security*, *87*, 101601. https://doi.org/10.1016/j.cose.2019.101601

Butavicius, M., Parsons, K., Pattinson, M., & McCormac, A. (2016). Breaching the human firewall: Social engineering in phishing and spear-phishing emails. *arXiv preprint arXiv:1606.00887*. https://arxiv.org/abs/1606.00887

Campbell, J., Greenauer, N., Macaluso, K., & End, C. (2007). Unrealistic optimism in internet events. *Computers in Human Behavior*, *23*(3), 1273-1284. https://doi.org/10.1016/j.chb.2004.12.005

Caputo, D. D., Pfleeger, S. L., Sasse, M. A., Ammann, P., Offutt, J., & Deng, L. (2016). Barriers to usable security? Three organizational case studies. *IEEE Security & Privacy*, *14*(5), 22-32. https://doi.org/10.1109/msp.2016.95

Carver, C. S., & Scheier, M. F. (2014). Dispositional optimism. *Trends in Cognitive Sciences*, *18*(6), 293-299. https://doi.org/10.1016/j.tics.2014.02.003

Cavaye, A. L. (1996). Case study research: a multi-faceted research approach for IS. *Information Systems Journal*, *6*(3), 227-242. https://doi.org/10.1111/j.1365-2575.1996.tb00015.x

Chambers, R., Tingey, L., Mullany, B., Parker, S., Lee, A., & Barlow, A. (2016). Exploring sexual risk taking among American Indian adolescents through protection motivation theory. *AIDS Care*, *28*(9), 1089-1096. https://doi.org/10.1080/09540121.2016.1164289

Chen, C. C., Shaw, R. S., & Yang, S. C. (2006). Mitigating information security risks by increasing user security awareness: A case study of an information security awareness system. *Information Technology, Learning & Performance Journal*, *24*(1). http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.102.5945&rep=rep1&type=pdf

Chen, H., Turel, O., & Yuan, Y. (2021). E-waste information security protection motivation: the role of optimism bias. *Information Technology & People*. Vol. ahead-of-print No. ahead-of-print. https://doi.org/10.1108/ITP-09-2019-0458

Chen, X., Wu, D., Chen, L., & Teng, J. K. (2018). Sanction severity and employees' information security policy compliance: Investigating mediating, moderating, and control variables. *Information & Management*, *55*(8), 1049-1060. https://doi.org/10.1016/j.im.2018.05.011

Chen, Y. (2017). Examining Internet Users' Adaptive and Maladaptive Security Behaviors Using the Extended Parallel Process Model. https://aisel.aisnet.org/icis2017/Security/Presentations/3/

Chen, Y., Galletta, D. F., Lowry, P. B., Luo, X., Moody, G. D., & Willison, R. (2021). Understanding Inconsistent Employee Compliance with Information Security Policies

Through the Lens of the Extended Parallel Process Model. *Information Systems Research*, *32*(3), 675-1097. https://doi.org/10.1287/isre.2021.1014

Chigada, J., & Madzinga, R. (2021). Cyberattacks and threats during COVID-19: A systematic literature review. *South African Journal of Information Management*, *23*(1), 1-11. https://doi.org/10.4102/sajim.v23i1.1277

Chmielarz, W., & Szumski, O. (2019). Cyber Security Patterns Students Behavior and Their Participation in Loyalty Programs. In *Cyber Law, Privacy, and Security: Concepts, Methodologies, Tools, and Applications* (pp. 1247-1263). IGI Global. https://doi.org/10.4018/978-1-5225-8897-9.ch061

Cho, H., Lee, J. S., & Chung, S. (2010). Optimistic bias about online privacy risks: Testing the moderating effects of perceived controllability and prior experience. *Computers in Human Behavior*, *26*(5), 987-995. https://doi.org/10.1016/j.chb.2010.02.012

Chua, Y. T., Parkin, S., Edwards, M., Oliveira, D., Schiffner, S., Tyson, G., & Hutchings, A. (2019, November). Identifying unintended harms of cybersecurity countermeasures. In *2019 APWG Symposium on Electronic Crime Research (eCrime)*(pp. 1-15). IEEE. https://doi.org/10.1109/ecrime47957.2019.9037589

Cismaru, M. (2006). Using protection motivation theory to increase the persuasiveness of public service communications. *Saskatchewan Institute of Public Policy Public Policy Series,* 1–27. https://policycommons.net/artifacts/1226987/using-protection-motivation-theory-to-increase-the-persuasiveness-of-public-service-communications/1780060/

Cline, R. J. W., Freeman, K. E., & Johnson, S. J. (1990). Talk among sexual partners about AIDS: Factors differentiating those who talk from those who do not. *Communication Research*, *17*(6), 792-808. https://doi.org/10.1177/009365029001700605

Coles-Kemp, L., & Hansen, R. R. (2017, July). Walking the line: The everyday security ties that bind. In *International Conference on Human Aspects of Information Security, Privacy, and Trust* (pp. 464-480). Springer, Cham.

Coles-Kemp, L., & Jensen, R. B. (2019, May). Accessing a new land: Designing for a social conceptualisation of access. In *Proceedings of the 2019 CHI Conference on Human*

Factors in Computing Systems (pp. 1-12). https://doi.org/10.1007/978-3-319-58460-7_32

Cone, B. D., Irvine, C. E., Thompson, M. F., & Nguyen, T. D. (2007). A video game for cyber security training and awareness. *Computers & Security*, *26*(1), 63-72. https://doi.org/10.1016/j.cose.2006.10.005

Cone, B. D., Thompson, M. F., Irvine, C. E., & Nguyen, T. D. (2006). Cyber security training and awareness through game play. In *IFIP International Information Security Conference* (pp. 431-436). Springer, Boston, MA. https://doi.org/10.1007/0-387-33406-8_37

Conner, M., & Sparks, P. (2005). Theory of planned behaviour and health behaviour. *Predicting Health Behaviour*, *2*(1), 121-162. https://doi.org/10.1348/135910705x43741

Conversano, C., Rotondo, A., Lensi, E., Della Vista, O., Arpone, F., & Reda, M. A. (2010). Optimism and its impact on mental and physical well-being. *Clinical practice and epidemiology in mental health: CP & EMH*, *6*, 25. https://doi.org/10.2174/1745017901006010025

Coombs, W. T., & Holladay, S. J. (2009). Further explorations of post-crisis communication: Effects of media and response strategies on perceptions and intentions. *Public Relations Review*, *35*(1), 1-6. https://doi.org/10.1016/j.pubrev.2008.09.011

Corradini I. (2020). Redefining the approach to cybersecurity. In: *Building a cybersecurity culture in organizations*. Cham: Springer. p. 49–62. https://doi.org/10.1007/978-3-030-43999-6_3

Covello, V. T., McCallum, D. B., & Pavlova, M. (1989). Principles and guidelines for improving risk communication. In *Effective risk communication* (pp. 3-16). Springer, Boston, MA. https://doi.org/10.1007/978-1-4613-1569-8_1

Coventry, L., Briggs, P., Jeske, D., & van Moorsel, A. (2014, June). SCENE: A structured means for creating and evaluating behavioral nudges in a cyber security environment. In *International conference of design, user experience, and usability* (pp. 229-239). Springer, Cham. https://doi.org/10.1007/978-3-319-07668-3_23

Crossland, G. C., & Ertan, A. (2021, June). Remote Working and (In)Security. *The Research Institute for Sociotechnical Cyber Security.* https://www.riscs.org.uk/wp-content/uploads/2021/07/RemoteWorking.pdf

Crozier, R. (2018). *DLA Piper paid 15,000 hours of IT overtime after NotPetya attack*. iTnews. https://www.itnews.com.au/news/dla-piper-paid-15000-hours-of-it-overtime-after-notpetya-attack-490495.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security*, *32*, 90-101. https://doi.org/10.1016/j.cose.2012.09.010

Crowe, S., Cresswell, K., Robertson, A., Huby, G., Avery, A., & Sheikh, A. (2011). The case study approach. *BMC medical research methodology*, *11*(1), 1-9. https://doi.org/10.1186/1471-2288-11-100

Cyber Security Breaches Survey 2020. GOV.UK. (2020). https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2020/cyber-security-breaches-survey-2020.

Czosseck, C., Ottis, R., & Talihärm, A. M. (2011). Estonia after the 2007 cyber attacks: Legal, strategic and organisational changes in cyber security. *International Journal of Cyber Warfare and Terrorism (IJCWT)*, *1*(1), 24-34. https://doi.org/10.4018/ijcwt.2011010103

D'Arcy, J., & Greene, G. (2014). Security culture and the employment relationship as drivers of employees' security compliance. *Information Management and Computer Security*, *22*(5), 474-489. https://doi.org/10.1108/imcs-08-2013-0057

D'Arcy, J., Herath, T., & Shoss, M. K. (2014). Understanding employee responses to stressful information security requirements: A coping perspective. *Journal of Management Information Systems*, *31*(2), 285-318. https://doi.org/10.2753/mis0742-1222310210

Da Silva, J. (2021). Producing 'good enough automated transcripts securely: Extending Bokhove and Downey (2018) to address security concerns. *Methodological Innovations*, *14*(1), 2059799120987766. https://doi.org/10.1177/2059799120987766

Da Silva, J. (2022). Cyber security and the Leviathan. *Computers & Security*, 116, 102674. https://doi.org/10.1016/j.cose.2022.102674

Da Silva, J., & Jensen, R. B. (2022). 'Cyber security is a dark art': The CISO as soothsayer. *arXiv preprint arXiv:2202.12755.* https://doi.org/10.48550/arXiv.2202.12755

Da Veiga, A. (2016). Comparing the information security culture of employees who had read the information security policy and those who had not: Illustrated through an empirical study. *Information & Computer Security, 24*(2), 139–151. https://doi.org/10.1108/ics-12-2015-0048

Da Veiga, A., & Eloff, J. H. (2010). A framework and assessment instrument for information security culture. *Computers & Security*, *29*(2), 196-207. https://doi.org/10.1016/j.cose.2009.09.002

Da Veiga, A., & Martins, N. (2015). Improving the information security culture through monitoring and implementation actions illustrated through a case study. *Computers & Security*, *49*, 162-176. https://doi.org/10.1016/j.cose.2014.12.006

Da Veiga, A., & Martins, N. (2017). Defining and identifying dominant information security cultures and subcultures. *Computers & Security*, *70*, 72-94. https://doi.org/10.1016/j.cose.2017.05.002

Dang-Pham, D., & Pittayachawan, S. (2015). Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university: A Protection Motivation Theory approach. *Computers & Security*, *48*, 281-297. https://doi.org/10.1016/j.cose.2014.11.002

DeJoy, D. M. (1989). The optimism bias and traffic accident risk perception. *Accident Analysis & Prevention*, *21*(4), 333-340. https://doi.org/10.1016/0001-4575(89)90024-9

DeJoy, D. M. (1992). An examination of gender differences in traffic accident risk perception. *Accident Analysis & Prevention*, *24*(3), 237-246. https://doi.org/10.1016/0001-4575(92)90003-2

Dekker, M., & Faber, M. J. (2008). Human security from below in a Hobbesian environment. *Security & Hum. Rts*, *19*, 37. https://doi.org/10.1163/187502308784048483

Dhillon, G., & Torkzadeh, G. (2006). Value-focused assessment of information system security in organizations. *Information Systems Journal*, *16*(3), 293-314. https://doi.org/10.1111/j.1365-2575.2006.00219.x

DiCicco-Bloom, B., & Crabtree, B. F. (2006). The qualitative research interview. *Medical Education, 40*(4), 314-321. https://doi.org/10.1111/j.1365-2929.2006.02418.x

Diefenbach, T. (2009). Are case studies more than sophisticated storytelling?: Methodological problems of qualitative empirical research mainly based on semi-structured interviews. *Quality & Quantity*, *43*(6), 875-894. https://doi.org/10.1007/s11135-008-9164-0

Dillard, A. J., Midboe, A. M., & Klein, W. M. (2009). The dark side of optimism: Unrealistic optimism about problems with alcohol predicts subsequent negative event experiences. *Personality and Social Psychology Bulletin*, *35*(11), 1540-1550. https://doi.org/10.1177/0146167209343124

Dillard, J. P. (1994). Rethinkin the study of fear appeals: An emotional perspective. *Communication Theory*, *4*(4), 295-323. https://doi.org/10.1111/j.1468-2885.1994.tb00094.x

Dilshad, R. M., & Latif, M. I. (2013). Focus group interview as a tool for qualitative research: An analysis. *Pakistan Journal of Social Sciences (PJSS)*, *33*(1), 191-198. https://doi.org/10.4135/9781506335179.n5

DiMaggio, P. (2013). Why cognitive (and cultural) sociology needs cognitive psychology. In *Culture in Mind* (pp. 271-278). Routledge.

Doane, A. N., Boothe, L. G., Pearson, M. R., & Kelley, M. L. (2016). Risky electronic communication behaviors and cyberbullying victimization: An application of Protection Motivation Theory. *Computers in Human Behavior*, *60*, 508-513. https://doi.org/10.1016/j.chb.2016.02.010

Dong, Y., Hu, S., & Zhu, J. (2018). From source credibility to risk perception: How and when climate information matters to action. *Resources, Conservation and Recycling*, *136*, 410-417. https://doi.org/10.1016/j.resconrec.2018.05.012

Dosman, D. M., Adamowicz, W. L., & Hrudey, S. E. (2001). Socioeconomic determinants of health-and food safety-related risk perceptions. *Risk Analysis*, *21*(2), 307-318. https://doi.org/10.1111/0272-4332.212113

Dourish, P., Grinter, R. E., De La Flor, J. D., & Joseph, M. (2004). Security in the wild: user strategies for managing security as an everyday, practical problem. *Personal and Ubiquitous Computing*, *8*(6), 391-401. https://doi.org/10.1007/s00779-004-0308-5

Duc-Bragues, C. (2015). Data Breaches and Privacy Law: Lawyers' Challenges in Handling Personal Information. *Cornell Law School J.D. Student Research Papers. Paper 35*. https://scholarship.law.cornell.edu/cgi/viewcontent.cgi?article=1050&context=lps_papers

Dunbar, N. E., Connelly, S., Jensen, M. L., Adame, B. J., Rozzell, B., Griffith, J. A., & Dan O'Hair, H. (2014). Fear appeals, message processing cues, and credibility in the websites of violent, ideological, and nonideological groups. *Journal of Computer-Mediated Communication*, *19*(4), 871-889. https://doi.org/10.1111/jcc4.12083

Dupuis, M., & Khan, F. (2018, May). Effects of peer feedback on password strength. In *2018 APWG Symposium on Electronic Crime Research (eCrime)* (pp. 1-9). IEEE. https://doi.org/10.1109/ecrime.2018.8376210

Durojaiye, T., Mersinas, K., & Watling, D. (2020). What Influences People's View of Cyber Security Culture in Higher Education Institutions? An Empirical Study. Available at: https://pure.royalholloway.ac.uk/portal/files/43620729/T_Durojaiye_K_Mersinas_D_Watling_2021_What_influence_people_s_views_of_Cyber_Security_Culture_CYBER21_.pdf

Egelman, S., Cranor, L. F., & Hong, J. (2008, April). You've been warned: an empirical study of the effectiveness of web browser phishing warnings. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 1065-1074). https://doi.org/10.1145/1357054.1357219

Einwiller, S. A., Laufer, D., & Ruppel, C. (2017). Believe me, I am one of you! The role of common group affiliation in crisis communication. *Public Relations Review*, *43*(5), 1007-1015. https://doi.org/10.1016/j.pubrev.2017.09.006

Eisenhardt, K. M. (1989). Building theories from case study research. *Academy of Management Review*, *14*(4), 532-550. https://doi.org/10.5465/amr.1989.4308385

Eisenman, D. P., Cordasco, K. M., Asch, S., Golden, J. F., & Glik, D. (2007). Disaster planning and risk communication with vulnerable communities: lessons from Hurricane Katrina. *American Journal of Public Health*, *97*(Supplement_1), S109-S115. https://doi.org/10.2105/ajph.2005.084335

Elder, R. W., Shults, R. A., Sleet, D. A., Nichols, J. L., Thompson, R. S., Rajab, W., & Task Force on Community Preventive Services. (2004). Effectiveness of mass media campaigns for reducing drinking and driving and alcohol-involved crashes: a systematic review. *American Journal of Preventive Medicine*, *27*(1), 57-65. https://doi.org/10.1016/j.amepre.2004.03.002

Eminağaoğlu, M., Uçar, E., & Eren, Ş. (2009). The positive outcomes of information security awareness training in companies–A case study. *Information Security Technical Report*, *14*(4), 223-229. https://doi.org/10.1016/j.istr.2010.05.002

Engbers, L. H., van Poppel, M. N., Paw, M. J. C. A., & van Mechelen, W. (2005). Worksite health promotion programs with environmental changes: a systematic review. *American Journal of Preventive Medicine*, *29*(1), 61-70. https://doi.org/10.1016/j.amepre.2005.03.001

Epton, T., Harris, P. R., Kane, R., van Koningsbruggen, G. M., & Sheeran, P. (2015). The impact of self-affirmation on health-behavior change: A meta-analysis. *Health Psychology*, *34*(3), 187-196. https://doi.org/10.1037/hea0000116

Ertan, A., Crossland, G., Heath, C., Denny, D., & Jensen, R. (2020). Cyber security behaviour in organisations. *arXiv preprint arXiv:2004.11768*. https://doi.org/10.48550/arXiv.2004.11768

Etheridge, B., Tang, L., & Wang, Y. (2020). Worker productivity during lockdown and working from home: Evidence from self-reports. *Covid Economics*, *52*, 118-151. https://doi.org/10.2139/ssrn.3643890

Etsebeth, V. (2006, July). Information Security Policies-The Legal Risk of Uninformed Personnel. In *ISSA* (pp. 1-10). https://www.academia.edu/download/46833968/104_Paper.pdf

Fauville, G., Luo, M., Muller Queiroz, A. C., Bailenson, J. N., & Hancock, J. (2021). Nonverbal Mechanisms Predict Zoom Fatigue and Explain Why Women Experience Higher Levels than Men. *Available at SSRN 3820035*. https://doi.org/10.2139/ssrn.3820035

Filipczuk, D., Mason, C., & Snow, S. (2019, May). Using a game to explore notions of responsibility for cyber security in organisations. In *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems* (pp. 1-6). https://doi.org/10.1145/3290607.3312846

Financial Times. (2017). DLA Piper still struggling with Petya cyber attack. https://www.ft.com/content/1b5f863a-624c-11e7-91a7-502f7ee26895.

Fischhoff, B. (1995). Risk perception and communication unplugged: Twenty years of process 1. *Risk Analysis*, *15*(2), 137-145. https://doi.org/10.1111/j.1539-6924.1995.tb00308.x

Flechais, I., Riegelsberger, J., & Sasse, M. A. (2005, September). Divide and conquer: the role of trust and assurance in the design of secure socio-technical systems. In *Proceedings of the 2005 workshop on New Security Paradigms* (pp. 33-41). https://doi.org/10.1145/1146269.1146280

Flick, C., Fisk, M., & Ogoh, G. (2020). Engaging Small and Medium-Sized Enterprises in Responsible Innovation. *Responsible Innovation*, 71-83. https://doi.org/10.1007/978-94-024-1720-3_6

Flores, W. R., & Ekstedt, M. (2016). Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. *Computers & Security, 59*, 26-44. https://doi.org/10.1016/j.cose.2016.01.004

Flores, W. R., Holm, H., Nohlberg, M., & Ekstedt, M. (2015). Investigating personal determinants of phishing and the effect of national culture. *Information & Computer Security*, *23*(2), 178-199. https://doi.org/10.1108/ics-05-2014-0029

Flores, W. R., Holm, H., Svensson, G., & Ericsson, G. (2014). Using phishing experiments and scenario-based surveys to understand security behaviours in practice. *Information*

Management & Computer Security, *22(*4), 393-406. https://doi.org/10.1108/imcs-11-2013-0083

Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A meta-analysis of research on protection motivation theory. *Journal of Applied Social Psychology*, *30*(2), 407-429. https://doi.org/10.1111/j.1559-1816.2000.tb02323.x

Flynn, J., Slovic, P., & Mertz, C. K. (1994). Gender, race, and perception of environmental health risks. *Risk Analysis*, *14*(6), 1101-1108. https://doi.org/10.1111/j.1539-6924.1994.tb00082.x

Flyvbjerg, B., Glenting, C., & Rønnest, A. (2004). Procedures for dealing with optimism bias in transport planning. *London: The British Department for Transport, Guidance Document*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2278346

Folkes, V. S. (1988). The availability heuristic and perceived risk. *Journal of Consumer Research*, *15*(1), 13-23. https://doi.org/10.1086/209141

Forstenlechner, I., Lettice, F., & Tschida, M. (2009). "Fee earner vs fee burner": internal divides in law firms. *Employee Relations, 31*(1), 98-113. https://doi.org/10.1108/01425450910916841

Freitas, H., Oliveira, M., Jenkins, M., & Popjoy, O. (1998). The Focus Group, a qualitative research method. *Journal of Education*, *1*(1), 1-22. https://www.ufrgs.br/gianti/files/artigos/1998/1998_079_ISRC.pdf

Friedman, L. C., Webb, J. A., Bruce, S., Weinberg, A. D., & Cooper, H. P. (1995). Skin cancer prevention and early detection intentions and behavior. *American Journal of Preventive Medicine*, *11*(1), 59-65. https://doi.org/10.1016/s0749-3797(18)30502-6

Furnell, S. M., Bryant, P., & Phippen, A. D. (2007). Assessing the security perceptions of personal Internet users. *Computers & Security*, *26*(5), 410-417. https://doi.org/10.1016/j.cose.2007.03.001

Furnell, S., & Clarke, N. (2012). Power to the people? The evolving recognition of human aspects of security. *Computers & Security*, *31*(8), 983-988. https://doi.org/10.1016/j.cose.2012.08.004

Furnell, S., & Shah, J. N. (2020). Home working and cyber security–an outbreak of unpreparedness?. *Computer Fraud & Security*, *2020*(8), 6-12. https://doi.org/10.1016/s1361-3723(20)30084-1

Gabriel, T., & Furnell, S. (2011). Selecting security champions. *Computer Fraud & Security*, *2011*(8), 8-12. https://doi.org/10.1016/s1361-3723(11)70082-3

Gambino, A., Kim, J., Sundar, S. S., Ge, J., & Rosson, M. B. (2016, May). User disbelief in privacy paradox: Heuristics that determine disclosure. In *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems* (pp. 2837-2843). https://doi.org/10.1145/2851581.2892413

Genge, B., Kiss, I., & Haller, P. (2015). A system dynamics approach for assessing the impact of cyber attacks on critical infrastructures. *International Journal of Critical Infrastructure Protection*, *10*(1), 3-17. https://doi.org/10.1016/j.ijcip.2015.04.001

Marangunić, N., & Granić, A. (2015). Technology acceptance model: a literature review from 1986 to 2013. *Universal access in the information society*, *14*(1), 81-95. https://doi.org/10.1007/s10209-014-0348-1

Gentner, D., & Stevens, A. L. (Eds.). (2014). *Mental Models*. Psychology Press. https://doi.org/10.4324/9781315802725

Georgescu, T. M. (2021). A Study on how the Pandemic Changed the Cybersecurity Landscape. *Informatica Economica*, *25*(1), 42-60. https://doi.org/10.24818/issn14531305/25.1.2021.04

Georgiadou, A., Mouzakitis, S., & Askounis, D. (2021). Working from home during COVID-19 crisis: a cyber security culture assessment survey. *Security Journal*, 1-20. https://doi.org/10.1057/s41284-021-00286-2

Ghafur, S., Grass, E., Jennings, N. R., & Darzi, A. (2019). The challenges of cybersecurity in health care: the UK National Health Service as a case study. *The Lancet Digital Health*, *1*(1), e10-e12. https://doi.org/10.1016/s2589-7500(19)30005-6

Gilovich, T., Griffin, D., & Kahneman, D. (Eds.). (2002). *Heuristics and biases: The psychology of intuitive judgment*. Cambridge university press. https://doi.org/10.1017/cbo9780511808098

Gioe, D. V., Goodman, M. S., & Wanless, A. (2019). Rebalancing cybersecurity imperatives: patching the social layer. *Journal of Cyber Policy*, *4*(1), 117-137. https://doi.org/10.1080/23738871.2019.1604780

Glanznig, M. (2012). User experience research: Modelling and describing the subjective. *Interdisciplinary Description of Complex Systems: INDECS*, *10*(3), 235-247. https://doi.org/10.7906/indecs.10.3.3

Glaspie, H. W., & Karwowski, W. (2017, July). Human factors in information security culture: A literature review. In *International Conference on Applied Human Factors and Ergonomics* (pp. 269-280). Springer, Cham. https://doi.org/10.1007/978-3-319-60585-2_25

Godin, G., & Kok, G. (1996). The theory of planned behavior: a review of its applications to health-related behaviors. *American Journal of Health Promotion*, *11*(2), 87-98. https://doi.org/10.4278/0890-1171-11.2.87

Goldstein, K. (2002). Getting in the door: Sampling and completing elite interviews. *PS: Political Science & Politics*, *35*(4), 669-672. https://doi.org/10.1017/s1049096502001130

Goo, J., Yim, M. S., & Kim, D. J. (2014). A path to successful management of employee security compliance: An empirical study of information security climate. *IEEE Transactions on Professional Communication*, *57*(4), 286-308. https://doi.org/10.1109/tpc.2014.2374011

Goodwin, T. (2012). Why we should reject 'nudge'. *Politics*, *32*(2), 85-92. https://doi.org/10.1111/j.1467-9256.2012.01430.x

Gore, T. D., & Bracken, C. C. (2005). Testing the theoretical design of a health risk message: Reexamining the major tenets of the extended parallel process model. *Health Education & Behavior*, *32*(1), 27-41. https://doi.org/10.1177/1090198104266901

Gray, L. M., Wong-Wylie, G., Rempel, G. R., & Cook, K. (2020). Expanding qualitative research interviewing strategies: Zoom video communications. *The Qualitative Report*, *25*(5), 1292-1301. https://doi.org/10.46743/2160-3715/2020.4212

Gray, L., MacDonald, C., Mackie, B., Paton, D., Johnston, D., & Baker, M. G. (2012). Community responses to communication campaigns for influenza A (H1N1): a focus group study. *BMC Public Health*, *12*(1), 1-12. https://doi.org/10.1186/1471-2458-12-205

Grazioli, S. (2004). Where did they go wrong? An analysis of the failure of knowledgeable internet consumers to detect deception over the internet. *Group Decision and Negotiation*, *13*(2), 149-172. https://doi.org/10.1023/b:grup.0000021839.04093.5d

Green, M., & Smith, M. (2016). Developers are not the enemy!: The need for usable security apis. *IEEE Security & Privacy*, *14*(5), 40-46. https://doi.org/10.1109/msp.2016.111

Greenberg, A. (2018). The untold story of NotPetya, the most devastating cyberattack in history. *Wired.* Available at: https://qualityplusconsulting.com/BBytes/2018-8-22_NotPetya-TheMost%20DevastatingCyberattackInHistory.pdf

Groarke, J. M., Berry, E., Graham-Wisener, L., McKenna-Plumley, P. E., McGlinchey, E., & Armour, C. (2020). Loneliness in the UK during the COVID-19 pandemic: Cross-sectional results from the COVID-19 Psychological Wellbeing Study. *PLOS one*, *15*(9), e0239698. https://doi.org/10.1371/journal.pone.0239698

Gu, C., Chan, C. W., He, G. P., Choi, K. C., & Yang, S. B. (2013). Chinese women's motivation to receive future screening: the role of social-demographic factors, knowledge and risk perception of cervical cancer. *European Journal of Oncology Nursing*, *17*(2), 154-161. https://doi.org/10.1016/j.ejon.2012.04.005

Guest, G., Bunce, A., & Johnson, L. (2006). How many interviews are enough? An experiment with data saturation and variability. *Field Methods*, *18*(1), 59-82. https://doi.org/10.1177/1525822x05279903

Gupta, R., & Agarwal, S. P. (2017). A comparative study of cyber threats in emerging economies. *Globus: An International Journal of Management & IT*, *8*(2), 24-28. https://doi.org/10.1108/jmtm-09-2016-0123

Haag, S., Siponen, M., & Liu, F. (2021). Protection Motivation Theory in Information Systems Security Research: A Review of the Past and a Road Map for the Future. *ACM SIGMIS*

Database: the DATABASE for Advances in Information Systems, *52*(2), 25-67. https://doi.org/10.1145/3462766.3462770

Habib, H., Naeini, P. E., Devlin, S., Oates, M., Swoopes, C., Bauer, L., ... & Cranor, L. F. (2018). User behaviors and attitudes under password expiration policies. In *Fourteenth Symposium on Usable Privacy and Security ({SOUPS} 2018)*(pp. 13-30). https://www.usenix.org/conference/soups2018/presentation/habib-password

Hadlington, L. J. (2018). Employees attitudes towards cyber security and risky online behaviours: an empirical assessment in the United Kingdom. *International Journal of Cyber Criminology, 12*(1), 262–274. https://dora.dmu.ac.uk/handle/2086/16801

Haimes, Y. Y. (2009). On the complex definition of risk: A systems-based approach. *Risk Analysis: An International Journal*, *29*(12), 1647-1654. https://doi.org/10.1111/j.1539-6924.2009.01310.x

Halcomb, E. J., & Davidson, P. M. (2006). Is verbatim transcription of interview data always necessary?. *Applied Nursing Research*, *19*(1), 38-42. https://doi.org/10.1016/j.apnr.2005.06.001

Halevi, T., Memon, N., Lewis, J., Kumaraguru, P., Arora, S., Dagar, N., ... & Chen, J. (2016, November). Cultural and psychological factors in cyber-security. In *Proceedings of the 18th International Conference on Information Integration and Web-based Applications and Services* (pp. 318-324). https://doi.org/10.1145/3011141.3011165

Haltinner, K., Sarathchandra, D., & Lichtenberg, N. (2015, April). Can I Live? College Student Perceptions of Risks, Security, and Privacy in Online Spaces. In *Cyber Security Symposium* (pp. 69-81). Springer, Cham. https://doi.org/10.1007/978-3-319-28313-5_6

Haney, J. M., & Lutters, W. G. (2018). " It's {Scary… It's}{Confusing… It's} Dull": How Cybersecurity Advocates Overcome Negative Perceptions of Security. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*(pp. 411-425). https://doi.org/10.1109/msec.2021.3077405

Hanus, B., & Wu, Y. A. (2016). Impact of users' security awareness on desktop security behavior: A protection motivation theory perspective. *Information Systems Management*, *33*(1), 2-16. https://doi.org/10.1080/10580530.2015.1117842

Haselton, M. G., Nettle, D., & Andrews, P. W. (2015). The evolution of cognitive bias. *The handbook of evolutionary psychology*, 724-746. https://doi.org/10.1002/9781119125563.evpsych241

Harris, P. R., & Napper, L. (2005). Self-affirmation and the biased processing of threatening health-risk information. *Personality and Social Psychology Bulletin*, *31*(9), 1250-1263. https://doi.org/10.1177/0146167205274694

Harris, P., Middleton, W., & Joiner, R. (2000). The typical student as an in-group member: eliminating optimistic bias by reducing social distance. *European Journal of Social Psychology*, *30*(2), 235-253. https://doi.org/10.1002/(sici)1099-0992(200003/04)30:2<235::aid-ejsp990>3.0.co;2-g

Harvey, N. (2007). Use of heuristics: Insights from forecasting research. *Thinking & Reasoning*, *13*(1), 5-24. https://doi.org/10.1080/13546780600872502

Harvey, W. S. (2011). Strategies for conducting elite interviews. *Qualitative Research*, *11*(4), 431-441. https://doi.org/10.1177/1468794111404329

Hassanzadeh, A., Rasekh, A., Galelli, S., Aghashahi, M., Taormina, R., Ostfeld, A., & Banks, M. K. (2020). A review of cybersecurity incidents in the water sector. *Journal of Environmental Engineering*, *146*(5), 03120003. https://doi.org/10.1061/(asce)ee.1943-7870.0001686

Heikkila, F. M. (2009). An analysis of the impact of information security policies on computer security breach incidents in law firms [Doctoral dissertation, Nova Southeastern University]. NSUworks. https://nsuworks.nova.edu/gscis_etd/176/

Heinonen, N. (2009). Flexible working and its implications for businesses: Case study IBM. https://www.theseus.fi/handle/10024/4247

Helweg-Larsen, M., Harding, H. G., & Klein, W. M. (2011). Will I divorce or have a happy marriage?: Gender differences in comparative optimism and estimation of personal

chances among US college students. *Basic and Applied Social Psychology*, *33*(2), 157-166. https://doi.org/10.1080/01973533.2011.568874

Herath, T., & Rao, H. R. (2009a). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems, 47*(2), 154-165. https://doi.org/10.1016/j.dss.2009.02.005

Herath, T., & Rao, H. R. (2009b). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems*, *18*(2), 106-125. https://doi.org/10.1057/ejis.2009.6

Herley, C. (2013). More is not the answer. *IEEE Security & Privacy*, *12*(1), 14-19. https://doi.org/10.1109/msp.2013.134

Hilbert, M. (2012). Toward a synthesis of cognitive biases: how noisy information processing can bias human decision making. *Psychological Bulletin*, *138*(2), 211. https://doi.org/10.1037/a0025940

Hofstede, G. (1998). Identifying organizational subcultures: An empirical approach. *Journal of Management Studies*, *35*(1), 1-12. https://doi.org/10.1037/a0025940

Holton, J. A. (2007). The coding process and its challenges. *The SAGE Handbook of Grounded Theory*, 265-289. https://doi.org/10.4135/9781848607941.n13

Hovav, A., & D'Arcy, J. (2012). Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the US and South Korea. *Information & Management*, *49*(2), 99-110. https://doi.org/10.1016/j.im.2011.12.005

Hovland, C. I., Janis, I. L., & Kelley, H. H. (1953). Communication and persuasion; psychological studies of opinion change. *American Sociological Review, (19)*3, 355-357. https://doi.org/10.2307/2087772

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences*, *43*(4), 615-660. https://doi.org/10.1111/j.1540-5915.2012.00361.x

Huang, D. L., Rau, P. L. P., Salvendy, G., Gao, F., & Zhou, J. (2011). Factors affecting perception of information security and their impacts on IT adoption and security

practices. *International Journal of Human-Computer Studies*, *69*(12), 870-883. https://doi.org/10.1016/j.ijhcs.2011.07.007

Hughes-Lartey, K., Li, M., Botchey, F. E., & Qin, Z. (2021). Human factor, a critical weak point in the information security of an organization's Internet of things. *Heliyon*, *7*(3), e06522. https://doi.org/10.1016/j.heliyon.2021.e06522

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, *31*(1), 83-95. https://doi.org/10.1016/j.cose.2011.10.007

Inglesant, P. G., & Sasse, M. A. (2010, April). The true cost of unusable password policies: password use in the wild. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 383-392). https://doi.org/10.1145/1753326.1753384

Iuga, C., Nurse, J. R., & Erola, A. (2016). Baiting the hook: factors impacting susceptibility to phishing attacks. *Human-centric Computing and Information Sciences*, *6*(1), 8-15. https://doi.org/10.1186/s13673-016-0065-2

Jakobsson, M., Tsow, A., Shah, A., Blevis, E., & Lim, Y. K. (2007, February). What instills trust? a qualitative study of phishing. In *International Conference on Financial Cryptography and Data Security* (pp. 356-361). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-77366-5_32

Jansen, L. A., Appelbaum, P. S., Klein, W. M., Weinstein, N. D., Cook, W., Fogel, J. S., & Sulmasy, D. P. (2011). Unrealistic optimism in early-phase oncology trials. *IRB*, *33*(1), 1. https://doi.org/10.1002/cncr.29908

Jansen, L. A., Mahadevan, D., Appelbaum, P. S., Klein, W. M., Weinstein, N. D., Mori, M., ... & Sulmasy, D. P. (2018). Perceptions of control and unrealistic optimism in early-phase cancer trials. *Journal of Medical Ethics*, *44*(2), 121-127. https://doi.org/10.1136/medethics-2016-103724

Jeong, J., Mihelcic, J., Oliver, G., & Rudolph, C. (2019, December). Towards an Improved Understanding of Human Factors in Cybersecurity. In *2019 IEEE 5th International*

Conference on Collaboration and Internet Computing (CIC)(pp. 338-345). IEEE. https://doi.org/10.1109/cic48465.2019.00047

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: an empirical study. *MIS Quarterly*, *34*(3), 549-566. https://doi.org/10.2307/25750691

Johnston, A. C., Wech, B., & Jack, E. (2000). Engaging remote employees: The moderating role of "remote" status in determining employee information security policy awareness. *Journal of Organizational and End User Computing (JOEUC)*, *25*(1), 1-23. https://doi.org/10.4018/joeuc.2013010101

Johnston, A. C., Wech, B., Jack, E., & Beavers, M. (2010). Reigning in the remote employee: Applying social learning theory to explain information security policy compliance attitudes. https://aisel.aisnet.org/amcis2010/493/

Joinson, A., & Steen, T. V. (2018). Human aspects of cyber security: Behaviour or culture change?. *Cyber Security: A Peer-Reviewed Journal*, *1*(4), 351-360. https://doi.org/10.1109/cybersecpods.2018.8560686

Jones, C. D., Newsome, J., Levin, K., Wilmot, A., McNulty, J. A., & Kline, T. (2018). Friends or strangers? A feasibility study of an innovative focus group methodology. *The Qualitative Report*, *23*(1), 98-112. https://doi.org/10.46743/2160-3715/2018.2940

Jonnalagadda, S., Bergamo, C., Lin, J. J., Lurslurchachai, L., Diefenbach, M., Smith, C., ... & Wisnivesky, J. P. (2012). Beliefs and attitudes about lung cancer screening among smokers. *Lung Cancer*, *77*(3), 526-531. https://doi.org/10.1016/j.lungcan.2012.05.095

Kahneman, D., Slovic, S. P., Slovic, P., & Tversky, A. (Eds.). (1982). *Judgment under uncertainty: Heuristics and biases*. Cambridge university press. https://doi.org/10.1515/9783112469187-009

Kang, R., Dabbish, L., Fruchter, N., & Kiesler, S. (2015). {"My} Data Just Goes {Everywhere:"} User Mental Models of the Internet and Implications for Privacy and Security. In *Eleventh Symposium on Usable Privacy and Security (SOUPS 2015)*(pp. 39-52). https://www.usenix.org/conference/soups2015/proceedings/presentation/kang

Karlsson, F., Åström, J., & Karlsson, M. (2015). Information security culture–state-of-the-art review between 2000 and 2013. *Information & Computer Security*, *23*(3), 246-285. https://doi.org/10.1108/ics-05-2014-0033

Katon, W. (2009). The impact of depression on workplace functioning and disability costs. *The American journal of managed care*, *15*(11 Suppl), S322-7.

Kerwin, J. T. (2012, March). 'Rational fatalism': non-monotonic choices in response to risks. In *Working Group in African Political Economy meeting, University of California, Berkeley, CA*. http://cega.berkeley.edu/assets/cega_events/49/Session_2A_HIV.pdf

Khalfan, A. M. (2004). Information security considerations in IS/IT outsourcing projects: a descriptive case study of two sectors. *International Journal of Information Management*, *24*(1), 29-42. https://doi.org/10.1016/j.ijinfomgt.2003.12.001

Khan, N. A., Brohi, S. N., & Zaman, N. (2020). Ten deadly cyber security threats amid COVID-19 pandemic. https://doi.org/10.36227/techrxiv.12278792

Kim, D. J., Phillps, B., & Ryu, Y. U. (2018, June). Impact of Perceived Risk, Perceived Controllability, and Security Self-Efficacy on Secure Intention from Social Comparison Theory Perspective. In *2018 National Cyber Summit (NCS)* (pp. 58-63). IEEE. https://doi.org/10.1109/ncs.2018.00014

Kim, H. K., & Niederdeppe, J. (2016). Effects of self-affirmation, narratives, and informational messages in reducing unrealistic optimism about alcohol-related problems among college students. *Human Communication Research*, *42*(2), 246-268. https://doi.org/10.1111/hcre.12073

Kim, H. L., & Han, J. (2019). Do employees in a "good" company comply better with information security policy? A corporate social responsibility perspective. *Information Technology & People*, *32*(4), 858-875. https://doi.org/10.1108/itp-09-2017-0298

Kim, J., & Mou, J. (2020). Meta-analysis of Information Security Policy Compliance Based on Theory of Planned Behavior. *Journal of Digital Convergence*, *18*(11), 169-176. https://doi.org/10.14400/JDC.2020.18.11.169

Kirlappos, I. (2016). *Learning from" shadow security": understanding non-compliant behaviours to improve information security management* (Doctoral dissertation, UCL (University College London)). https://discovery.ucl.ac.uk/id/eprint/1521997/

Kirlappos, I., & Sasse, M. A. (2011). Security education against phishing: A modest proposal for a major rethink. *IEEE Security & Privacy*, *10*(2), 24-32. https://doi.org/10.1109/msp.2011.179

Kirlappos, I., & Sasse, M. A. (2014, June). What usable security really means: Trusting and engaging users. In *International Conference on Human Aspects of Information Security, Privacy, and Trust* (pp. 69-78). Springer, Cham. https://doi.org/10.1007/978-3-319-07620-1_7

Kirlappos, I., Beautement, A., & Sasse, M. A. (2013, April). "Comply or Die" Is Dead: Long live security-aware principal agents. In *International conference on financial cryptography and data security* (pp. 70-82). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-41320-9_5

Kirlappos, I., Parkin, S., & Sasse, M. A. (2014). Learning from "Shadow Security": Why understanding non-compliance provides the basis for effective security. *Proceedings 2014 Workshop on Usable Security.* https://doi.org/10.14722/usec.2014.23007

Kirlappos, I., Parkin, S., & Sasse, M. A. (2015). " Shadow security" as a tool for the learning organization. *Acm Sigcas Computers and Society*, *45*(1), 29-37. https://doi.org/10.1145/2738210.2738216

Kirsch, L., & Boss, S. (2007). The last line of defense: motivating employees to follow corporate security guidelines. *ICIS 2007 proceedings*, 103. https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1260&context=icis2007

Kite, J., & Phongsavan, P. (2017). Insights for conducting real-time focus groups online using a web conferencing service. *F1000Research*, *6*(122), 1-12. https://doi.org/10.12688/f1000research.10427.1

Klein, W. M., & Kunda, Z. (1993). Maintaining self-serving social comparisons: Biased reconstruction of one's past behaviors. *Personality and Social Psychology Bulletin*, *19*(6), 732-739. https://doi.org/10.1177/0146167293196008

Klein, W. M., Lipkus, I. M., Scholl, S. M., McQueen, A., Cerully, J. L., & Harris, P. R. (2010). Self-affirmation moderates effects of unrealistic optimism and pessimism on reactions to tailored risk feedback. *Psychology and Health*, *25*(10), 1195-1208. https://doi.org/10.1080/08870440903261970

Knight, R., & Nurse, J. R. (2020). A framework for effective corporate communication after cyber security incidents. *Computers & Security*, *99*, 102036. https://doi.org/10.1016/j.cose.2020.102036

Kolkowska, E. (2011). Security subcultures in an organization-exploring value conflicts. *ECIS 2011 Proceedings. 237.* https://aisel.aisnet.org/ecis2011/237/

Koppel, R., Smith, S. W., Blythe, J., & Kothari, V. (2015). Workarounds to computer access in healthcare organizations: you want my password or a dead patient?. In *ITCH* (pp. 215-220). https://ebooks.iospress.nl/volumearticle/38745

Kraus, L., Fiebig, T., Miruchna, V., Möller, S., & Shabtai, A. (2015). Analyzing end-users' knowledge and feelings surrounding smartphone security and privacy. *S&P. IEEE*. http://www.ieee-security.org/TC/SPW2015/MoST/papers/s1p2.pdf

Krol, K., Spring, J. M., Parkin, S., & Sasse, M. A. (2016). Towards robust experimental design for user studies in security and privacy. In *The {LASER} Workshop: Learning from Authoritative Security Experiment Results ({LASER} 2016)* (pp. 21-31). https://www.usenix.org/conference/laser2016/program/presentation/krol

Kumaraguru, P., Cranshaw, J., Acquisti, A., Cranor, L., Hong, J., Blair, M. A., & Pham, T. (2009). School of phish: a real-world evaluation of anti-phishing training. In *Proceedings of the 5th Symposium on Usable Privacy and Security* (p. 3). ACM. https://doi.org/10.1145/1572532.1572536

Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L. F., Hong, J., & Nunge, E. (2007, April). Protecting people from phishing: the design and evaluation of an embedded training email system. In *Proceedings of the SIGCHI conference on Human Factors in Computing Systems* (pp. 905-914). ACM. https://doi.org/10.1145/1240624.1240760

Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L. F., & Hong, J. (2010). Teaching Johnny not to fall for phish. *ACM Transactions on Internet Technology (TOIT)*, *10*(2), 1-31. https://doi.org/10.1145/1754393.1754396

Kuypers, M. A., Maillart, T., & Paté-Cornell, E. (2016). An empirical analysis of cyber security incidents at a large organization. *Department of Management Science and Engineering, Stanford University, School of Information, UC Berkeley*. https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/kuypersweis_v7.pdf

Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security*, *105*, 102248. https://doi.org/10.1016/j.cose.2021.102248

Lawson, S. T., Yeo, S. K., Yu, H., & Greene, E. (2016, May). The cyber-doom effect: The impact of fear appeals in the US cyber security debate. In *2016 8th International Conference on Cyber Conflict (CyCon)* (pp. 65-80). IEEE. https://doi.org/10.1109/cycon.2016.7529427

Lebek, B., Uffen, J., Breitner, M. H., Neumann, M., & Hohler, B. (2013, January). Employees' information security awareness and behavior: A literature review. In *2013 46th Hawaii International Conference on System Sciences* (pp. 2978-2987). IEEE. https://doi.org/10.1109/hicss.2013.192

Lee, S. H., & Ham, E. M. (2010). The relationship between the optimistic bias about cancer and cancer preventive behavior of the Korean, Chinese, American, and Japanese adult residing in Korea. *Journal of Korean Academy of Nursing*, *40*(1), 52-59. https://doi.org/10.4040/jkan.2010.40.1.52

Leech, N. L., & Onwuegbuzie, A. J. (2011). Beyond constant comparison qualitative data analysis: Using NVivo. *School Psychology Quarterly*, *26*(1), 70-84. https://doi.org/10.1037/a0022711

Lehman, D. R., Chiu, C. Y., & Schaller, M. (2004). Psychology and culture. *Annu. Rev. Psychol.*, *55*, 689-714. https://doi.org/10.1146/annurev.psych.55.090902.141927

Leventhal, H. (1970). Findings and Theory in the Study of Fear Communications1. In *Advances in Experimental Social Psychology* (Vol. 5, pp. 119-186). Academic Press. https://doi.org/10.1016/s0065-2601(08)60091-x

Leventhal, H., & Trembly, G. (1968). Negative emotions and persuasion 1. *Journal of Personality*, *36*(1), 154-168. https://doi.org/10.1111/j.1467-6494.1968.tb01466.x

Lezaun, J. (2007). A market of opinions: the political epistemology of focus groups. *The Sociological Review*, *55*(2_suppl), 130-151. https://doi.org/10.1111/j.1467-954x.2007.00733.x

Liamputtong, P. (2011). Focus group methodology: Introduction and history. *Focus group methodology: Principle and Practice*, *224*(1), 1-14. https://doi.org/10.4135/9781473957657.n1

Lichtenstein, S., Slovic, P., Fischhoff, B., Layman, M., & Combs, B. (1978). Judged frequency of lethal events. *Journal of Experimental Psychology: Human Learning and Memory*, *4*(6), 551-578. https://doi.org/10.1037/0278-7393.4.6.551

Lika, R. A., Murugiah, D., Brohi, S. N., & Ramasamy, D. (2018, July). NotPetya: cyber attack prevention through awareness via gamification. In *2018 International Conference on Smart Computing and Electronic Enterprise (ICSCEE)* (pp. 1-6). IEEE. https://doi.org/10.1109/icscee.2018.8538431

Lindzey, G. E., & Aronson, E. E. (1968). *The Handbook of Social Psychology*. Reading, Mass., Addison-Wesley Pub. Co. https://doi.org/10.1086/287448

Lingard, L., & Watling, C. (2021). Effective Use of Quotes in Qualitative Research. In *Story, Not Study: 30 Brief Lessons to Inspire Health Researchers as Writers* (pp. 35-43). Springer, Cham. https://doi.org/10.1007/978-3-030-71363-8_6

Liu, N., Nikitas, A., & Parkinson, S. (2020). Exploring expert perceptions about the cyber security and privacy of Connected and Autonomous Vehicles: A thematic analysis approach. *Transportation research part F: traffic psychology and behaviour*, *75*(1), 66-86. https://doi.org/10.1016/j.trf.2020.09.019

Lobe, B., & Morgan, D. L. (2020). Assessing the effectiveness of video-based interviewing: a systematic comparison of video-conferencing based dyadic interviews and focus

groups. *International Journal of Social Research Methodology*, 1-12. https://doi.org/10.1080/13645579.2020.1785763

Lobe, B., Morgan, D., & Hoffman, K. A. (2020). Qualitative data collection in an era of social distancing. *International Journal of Qualitative Methods*, *19*, 1-8. https://doi.org/10.1177/1609406920937875

Loch, K. D., Carr, H. H., & Warkentin, M. E. (1992). Threats to information systems: today's reality, yesterday's understanding. *MIS Quarterly, 16*(2), 173-186. https://doi.org/10.2307/249574

Lofstedt, R. E. (2006). How can we make food risk communication better: where are we and where are we going?. *Journal of Risk Research*, *9*(8), 869-890. https://doi.org/10.1080/13669870601065585

Lorsch, J. W., & Chernak, A. (2006). *DLA Piper: Becoming a Global Firm*. Harvard Business School Publishing. https://hbsp.harvard.edu/product/407057-PDF-ENG

Loske, A., Widjaja, T., & Buxmann, P. (2013). Cloud Computing Providers' Unrealistic Optimism regarding IT Security Risks: A Threat to Users?. *Thirty Fourth International Conference on Information Systems* (pp. 1-20). http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.689.5333&rep=rep1&type=pdf

Lowe, A., Norris, A. C., Farris, A. J., & Babbage, D. R. (2018). Quantifying thematic saturation in qualitative data analysis. *Field Methods*, *30*(3), 191-207. https://doi.org/10.1177/1525822x17749386

Lowry, P. B., & Moody, G. D. (2015). Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organisational information security policies. *Information Systems Journal*, *25*(5), 433-463. https://doi.org/10.1111/isj.12043

Ludolph, R., & Schulz, P. J. (2018). Debiasing health-related judgments and decision making: a systematic review. *Medical Decision Making*, *38*(1), 3-13. https://doi.org/10.1177/0272989x17716672

Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology*, *19*(5), 469-479. https://doi.org/10.1016/0022-1031(83)90023-9

Manning, J. (2017). In vivo coding. *The International Encyclopedia of Communication Research Methods*, 1-2. https://doi.org/10.1002/9781118901731.iecrm0270

Martins, C., Oliveira, T., & Popovič, A. (2014). Understanding the Internet banking adoption: A unified theory of acceptance and use of technology and perceived risk application. *International Journal of Information Management*, *34*(1), 1-13. https://doi.org/10.1016/j.ijinfomgt.2013.06.002

Masiero, M., Riva, S., Oliveri, S., Fioretti, C., & Pravettoni, G. (2018). Optimistic bias in young adults for cancer, cardiovascular and respiratory diseases: A pilot study on smokers and drinkers. *Journal of Health Psychology*, *23*(5), 645-656. https://doi.org/10.1177/1359105316667796

Masuch, K., Hengstler, S., Schulze, L., & Trang, S. (2021, January). The Impact of Threat and Efficacy on Information Security Behavior: Applying an Extended Parallel Process Model to the Fear of Ransomware. In *Proceedings of the 54th Hawaii International Conference on System Sciences* (p. 6691). https://doi.org/10.24251/hicss.2021.803

Matheson, J. L. (2007). The Voice Transcription Technique: Use of Voice Recognition Software to Transcribe Digital Interview Data in Qualitative Research. *Qualitative Report*, *12*(4), 547-560. https://doi.org/10.46743/2160-3715/2007.1611

McAlaney, J., & Benson, V. (2020). Cybersecurity as a social phenomenon. In *Cyber Influence and Cognitive Threats* (pp. 1-8). Academic Press. https://doi.org/10.1016/b978-0-12-819204-7.00001-4

McAlaney, J., Taylor, J., & Faily, S. (2016). The social psychology of cybersecurity. *Psychologist*, *29*(9), 686-689. http://eprints.bournemouth.ac.uk/22052/1/mctf15.pdf

McAlanley, J., Thackray, H., & Taylor, J. (2016). The social psychology of cybersecurity. *The Psychologist, 29*(9), 686-690. https://doi.org/10.14236/ewic/hci2016.64

McCarthy, J., & Wright, P. (2004). Technology as experience. *interactions*, *11*(5), 42-43. https://doi.org/10.1145/1015530.1015549

McCrohan, K. F., Engel, K., & Harvey, J. W. (2010). Influence of awareness and training on cyber security. *Journal of Internet Commerce*, *9*(1), 23-41. https://doi.org/10.1080/15332861.2010.487415

McEachan, R. R. C., Conner, M., Taylor, N. J., & Lawton, R. J. (2011). Prospective prediction of health-related behaviours with the theory of planned behaviour: A meta-analysis. *Health Psychology Review*, *5*(2), 97-144. https://doi.org/10.1080/17437199.2010.521684

McGraw, A. P., Mellers, B. A., & Ritov, I. (2004). The affective costs of overconfidence. *Journal of Behavioral Decision Making*, *17*(4), 281-295. https://doi.org/10.1002/bdm.472

McMahan, S., Witte, K., & Meyer, J. A. (1998). The perception of risk messages regarding electromagnetic fields: extending the extended parallel process model to an unknown risk. *Health Communication*, *10*(3), 247-259. https://doi.org/10.1207/s15327027hc1003_4

Mc Mahon, C. (2020). In Defence of the Human Factor. *Frontiers in Psychology*, *11*, 1390. https://doi.org/10.3389/fpsyg.2020.01390

McNerney, M., & Papadopoulos, E. (2012). Hacker's Delight: Law Firm Risk and Liability in the Cyber Age. *Am. UL Rev.*, *62*, 1243. https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/aulr62&section=39

McSweeney, B., McSweeney, W., & Bill, M. (1999). *Security, identity and interests: a sociology of international relations*(No. 69). Cambridge University Press. https://www.google.co.uk/books/edition/Security_Identity_and_Interests/VQVTa-CKLjUC?hl=en&gbpv=0

Menard, P., Bott, G. J., & Crossler, R. E. (2017). User Motivations in Protecting Information Security: Protection Motivation Theory Versus Self-Determination Theory. *Journal of Management Information Systems, 34*(4), 1203-1230. https://doi.org/10.1080/07421222.2017.1394083

Meyer, C. B. (2001). A case in case study methodology. *Field Methods*, *13*(4), 329-352. https://doi.org/10.1177/1525822x0101300402

Mezulis, A. H., Abramson, L. Y., Hyde, J. S., & Hankin, B. L. (2004). Is there a universal positivity bias in attributions? A meta-analytic review of individual, developmental, and cultural differences in the self-serving attributional bias. *Psychological Bulletin*, *130*(5), 711-747. https://doi.org/10.1037/0033-2909.130.5.711

Miao, P., Li, X., & Xie, X. (2020). Hard to bear: State boredom increases financial risk taking. *Social Psychology, 51*(3), 157–170. https://doi.org/10.1027/1864-9335/a000408

Milena, Z. R., Dainora, G., & Alin, S. (2008). Qualitative research methods: A comparison between focus-group and in-depth interview. *Annals of the University of Oradea, Economic Science Series*, *17*(4), 1279-1283. https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.458.3583&rep=rep1&type=pdf

Miles, M. B., & Huberman, A. M. (1994). *Qualitative data analysis: An expanded sourcebook*. sage. https://www.google.co.uk/books/edition/Qualitative_Data_Analysis/U4lU_-wJ5QEC?hl=en&gbpv=1&dq=Miles,+M.+B.,+%26+Huberman,+A.+M.+(1994).+Qualitative+data+analysis:+An+expanded+sourcebook.+sage.&pg=PA10&printsec=frontcover

Miles, R. (2015). Complexity, representation and practice: Case study as method and methodology. *Issues in Educational Research*, *25*(3), 309-318. http://www.iier.org.au/iier25/miles.html

Milne, S., Orbell, S., & Sheeran, P. (2002). Combining motivational and volitional interventions to promote exercise participation: Protection motivation theory and implementation intentions. *British Journal of Health Psychology*, *7*(2), 163-184. https://doi.org/10.1348/135910702169420

Milne, S., Sheeran, P., & Orbell, S. (2000). Prediction and intervention in health-related behavior: A meta-analytic review of protection motivation theory. *Journal of Applied Social Psychology*, *30*(1), 106-143. https://doi.org/10.1111/j.1559-1816.2000.tb02308.x

Mohamed, M. A., Chakraborty, J., & Dehlinger, J. (2017). Trading off usability and security in user interface design through mental models. *Behaviour & Information Technology*, *36*(5), 493-516. https://doi.org/10.1080/0144929x.2016.1262897

Molotch, H. (2013). Everyday security: Default to decency. *IEEE Security & Privacy*, *11*(6), 84-87. https://doi.org/10.1109/msp.2013.142

Monteith, S., Bauer, M., Alda, M., Geddes, J., Whybrow, P. C., & Glenn, T. (2021). Increasing Cybercrime Since the Pandemic: Concerns for Psychiatry. *Current Psychiatry Reports*, *23*(4), 1-9. https://doi.org/10.1007/s11920-021-01228-w

Moore, R. J. (2015). Automated transcription and conversation analysis. *Research on Language and Social Interaction*, *48*(3), 253-270. https://doi.org/10.1080/08351813.2015.1058600

Morgan, M. G., Fischhoff, B., Bostrom, A., & Atman, C. J. (2002). *Risk communication: A mental models approach*. Cambridge University Press. https://doi.org/10.1017/cbo9780511814679

Morgan, P. L., Asquith, P. M., Bishop, L. M., Raywood-Burke, G., Wedgbury, A., & Jones, K. (2020, July). A New Hope: Human-Centric Cybersecurity Research Embedded Within Organizations. In *International Conference on Human-Computer Interaction* (pp. 206-216). Springer, Cham. https://doi.org/10.1007/978-3-030-50309-3_14

Mubarak, S., & Slay, J. (2006, December). An explorative study on information security of trust accounts within law firms in South Australia: Implications for IT security management. In *2006 1st International Conference on Digital Information Management* (pp. 55-62). IEEE. https://doi.org/10.1109/icdim.2007.369330

Muendo, D. (2014). Information Security Subcultures in Information Security Management: A Conceptual Framework. *European Journal of Business and Management*, *6*(38), 1-8. https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.735.5272&rep=rep1&type=pdf

Mulilis, J. P., & Lippa, R. (1990). Behavioral change in earthquake preparedness due to negative threat appeals: A test of protection motivation theory. *Journal of Applied*

Social Psychology, *20*(8), 619-638. https://doi.org/10.1111/j.1559-1816.1990.tb00429.x

Mustajab, D., Bauw, A., Rasyid, A., Irawan, A., Akbar, M. A., & Hamid, M. A. (2020). Working from home phenomenon as an effort to prevent COVID-19 attacks and its impacts on work productivity. *TIJAB (The International Journal of Applied Business)*, *4*(1), 13-21. https://doi.org/10.20473/tijab.v4.i1.2020.13-21

Muthuppalaniappan, M., & Stevenson, K. (2021). Healthcare cyber-attacks and the COVID-19 pandemic: an urgent threat to global health. *International Journal for Quality in Health Care*, *33*(1), mzaa117. https://doi.org/10.1093/intqhc/mzaa117

Naidoo, R. (2020). A multi-level influence model of COVID-19 themed cybercrime. *European Journal of Information Systems*, *29*(3), 306-321. https://doi.org/10.1080/0960085x.2020.1771222

Nam, T. (2019). Understanding the gap between perceived threats to and preparedness for cybersecurity. *Technology in Society*, *58*, 101122. https://doi.org/10.1016/j.techsoc.2019.03.005

Nasir, A., Abdullah Arshah, R., & Ab Hamid, M. R. (2019). A dimension-based information security culture model and its relationship with employees' security behavior: A case study in Malaysian higher educational institutions. *Information Security Journal: A Global Perspective*, *28*(3), 55-80. https://doi.org/10.1080/19393555.2019.1643956

National Cyber Security Centre. (2021). *NCSC Annual Review 2021.* https://www.ncsc.gov.uk/collection/ncsc-annual-review-2021

Newington, L., & Metcalfe, A. (2014). Factors influencing recruitment to research: qualitative study of the experiences and perceptions of research teams. *BMC Medical Research Methodology*, *14*(1), 1-11. https://doi.org/10.1186/1471-2288-14-10

Niederdeppe, J., & Levy, A. G. (2007). Fatalistic beliefs about cancer prevention and three prevention behaviors. *Cancer Epidemiology and Prevention Biomarkers*, *16*(5), 998-1003. https://doi.org/10.1158/1055-9965.epi-06-0608

Norman, D. A. (2013). *The design of everyday things*. MIT Press. https://doi.org/10.15358/9783800648108

Norman, D. A. (1988). *The psychology of everyday things*. Basic books. https://doi.org/10.2307/3106094

Norman, P., Boer, H., & Seydel, E. R. (2005). Protection motivation theory. *Predicting Health Behaviour*, *81*, 126. https://doi.org/10.1348/135910703762879219

Novick, G. (2008). Is there a bias against telephone interviews in qualitative research?. *Research in Nursing & Health*, *31*(4), 391-398. https://doi.org/10.1002/nur.20259

Nurse, J. R. (2013, January). Effective communication of cyber security risks. In *7th International Scientific Conference on Security and Protection of Information (SPI 2013)*. https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.1068.4300&rep=rep1&type=pdf

Nurse, J. R., Creese, S., Goldsmith, M., & Lamberts, K. (2011a, September). Guidelines for usable cybersecurity: Past and present. In *2011 Third International Workshop on Cyberspace Safety and Security (CSS)* (pp. 21-26). IEEE. https://doi.org/10.1109/css.2011.6058566

Nurse, J. R., Creese, S., Goldsmith, M., & Lamberts, K. (2011b, September). Trustworthy and effective communication of cybersecurity risks: A review. In *2011 1st Workshop on Socio-Technical Aspects in Security and Trust (STAST)* (pp. 60-68). IEEE. https://doi.org/10.1109/stast.2011.6059257

Nurse, J. R., Williams, N., Collins, E., Panteli, N., Blythe, J., & Koppelman, B. (2021, July). Remote working pre-and post-COVID-19: an analysis of new threats and risks to security and privacy. In *International Conference on Human-Computer Interaction* (pp. 583-590). Springer, Cham. https://doi.org/10.1007/978-3-030-78645-8_74

O'leary, A., Jemmott, L. S., & Jemmott III, J. B. (2008). Mediation analysis of an effective sexual risk-reduction intervention for women: the importance of self-efficacy. *Health Psychology*, *27*(2S), S180. https://doi.org/10.1037/0278-6133.27.2(suppl.).s180

Oliveira, D., Rocha, H., Yang, H., Ellis, D., Dommaraju, S., Muradoglu, M., ... & Ebner, N. (2017, May). Dissecting spear phishing emails for older vs young adults: On the interplay of

weapons of influence and life domains in predicting susceptibility to phishing. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (pp. 6412-6424). https://doi.org/10.1145/3025453.3025831

Osborn, E., & Simpson, A. (2017). On small-scale IT users' system architectures and cyber security: A UK case study. *Computers & Security*, *70*, 27-50. https://doi.org/10.1016/j.cose.2017.05.001

Oxford University Press. (n.d.). *Oxford Advanced Learner's Dictionary*. Retrieved October 9, 2022, from https://www.oxfordlearnersdictionaries.com/

Pahnila, S., Siponen, M., & Mahmood, A. (2007, January). Employees' behavior towards IS security policy compliance. In *System sciences, 2007. HICSS 2007. 40Th annual hawaii international conference on* (pp. 156b-156b). IEEE. https://doi.org/10.1109/hicss.2007.206

Palenchar, M. J., & Heath, R. L. (2007). Strategic risk communication: Adding value to society. *Public Relations Review*, *33*(2), 120-129. https://doi.org/10.1016/j.pubrev.2006.11.014

Paliszkiewicz, J. (2019). Information security policy compliance: Leadership and trust. *Journal of Computer Information Systems*, *59*(3), 211-217.

Parker, D., Manstead, A. S., Stradling, S. G., Reason, J. T., & Baxter, J. S. (1992). Intention to commit driving violations: An application of the theory of planned behavior. *Journal of Applied Psychology*, *77*(1), 94. https://doi.org/10.1080/08874417.2019.1571459

Parkin, S., Van Moorsel, A., Inglesant, P., & Sasse, M. A. (2010, September). A stealth approach to usable security: helping IT security managers to identify workable security solutions. In *Proceedings of the 2010 New Security Paradigms Workshop* (pp. 33-50). https://doi.org/10.1145/1900546.1900553

Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., & Jerram, C. (2014). A study of information security awareness in Australian government organisations. *Information Management & Computer Security*, *22*(4), 334-345. https://doi.org/10.1108/imcs-10-2013-0078

Pattinson, M., Jerram, C., Parsons, K., McCormac, A., & Butavicius, M. (2012). Why do some people manage phishing e-mails better than others?. *Information Management & Computer Security*, *20*(1), 18-28. https://doi.org/10.1108/09685221211219173

Pechmann, C., Zhao, G., Goldberg, M. E., & Reibling, E. T. (2003). What to convey in antismoking advertisements for adolescents: The use of protection motivation theory to identify effective message themes. *Journal of Marketing*, *67*(2), 1-18. https://doi.org/10.1509/jmkg.67.2.1.18607

Penney, J. (2019). The right to privacy: The end of Privacy Fatalism. In *Human Rights, Digital Society and the Law* (pp. 44-57). Routledge. https://doi.org/10.4324/9781351025386-4

Peters, E., McCaul, K. D., Stefanek, M., & Nelson, W. (2006). A heuristics approach to understanding cancer risk perception: contributions from judgment and decision-making research. *Annals of Behavioral Medicine*, *31*(1), 45-52. https://doi.org/10.1207/s15324796abm3101_8

Peters, G. J. Y., Ruiter, R. A., & Kok, G. (2013). Threatening communication: a critical re-analysis and a revised meta-analytic test of fear appeal theory. *Health Psychology Review*, *7*(sup1), S8-S31. https://doi.org/10.1080/17437199.2012.703527

Pettigrew, T. F. (2018). The emergence of contextual social psychology. *Personality and Social Psychology Bulletin*, *44*(7), 963-971. https://doi.org/10.1177/0146167218756033

Pham, H., Brennan, L., & Richardson, J. (2017, June). Review of behavioural theories in security compliance and research challenge. In *Informing Science and Information Technology Education Conference, Vietnam* (pp. 65-76). Santa Rosa, CA: Informing Science Institute. https://doi.org/10.28945/3722

Plough, A., & Krimsky, S. (1987). The emergence of risk communication studies: social and political context. *Science, Technology, & Human Values*, *12*(4), 4-10. https://www.jstor.org/stable/689375

Podsakoff, P. M., MacKenzie, S. B., Lee, J. Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: a critical review of the literature and recommended

remedies. *Journal of Applied Psychology*, *88*(5), 879-903. https://doi.org/10.1037/0021-9010.88.5.879

Poland, B. D. (2002). Transcription quality. *Handbook of interview research: Context and Method*, 629-649. https://doi.org/10.4135/9781412973588.n36

Ponemon Institute LLC. (August, 2021). *The State of Threat Hunting and the Role of the Analyst.* https://team-cymru.com/wp-content/uploads/2021/08/Ponemon_State-of-Threat-Hunting-Role-of-Analyst_Report_August-2021.pdf

Popova, L. (2012). The extended parallel process model: Illuminating the gaps in research. *Health Education & Behavior*, *39*(4), 455-473. https://doi.org/10.1177/1090198111418108

Posey, C., Roberts, T. L., Lowry, P. B., & Hightower, R. T. (2014). Bridging the divide: A qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders. *Information & Management*, *51*(5), 551-567. https://doi.org/10.1016/j.im.2014.03.009

Posey, C., Roberts, T., Lowry, P. B., Courtney, J., & Bennett, B. (2011, September). Motivating the insider to protect organizational information assets: Evidence from protection motivation theory and rival explanations. In *The Dewald Roode workshop in information systems security* (pp. 22-23). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2273594

Pranggono, B., & Arabo, A. (2021). COVID-19 pandemic cybersecurity issues. *Internet Technology Letters*, *4*(2), e247. https://doi.org/10.1002/itl2.247

Prentice-Dunn, S., & Rogers, R. W. (1986). Protection motivation theory and preventive health: Beyond the health belief model. *Health Education Research*, *1*(3), 153-161. https://doi.org/10.1093/her/1.3.153

Prince, M., & Davies, M. (2001). Moderator teams: an extension to focus group methodology. *Qualitative Market Research: An International Journal*, *4*(4), 207-216. https://doi.org/10.1108/eum0000000005902

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: an action research study. *Mis Quarterly, 34*(4), 757-778. https://doi.org/10.2307/25750704

Ramo, D. E., Meacham, M., Thrul, J., Belohlavek, A., Sarkar, U., & Humfleet, G. (2019). Exploring identities and preferences for intervention among LGBTQ+ young adult smokers through online focus groups. *Journal of Adolescent Health*, *64*(3), 390-397. https://doi.org/10.1016/j.jadohealth.2018.09.022

Rantos, K., Fysarakis, K., & Manifavas, C. (2012). How effective is your security awareness program? An evaluation methodology. *Information Security Journal: A Global Perspective*, *21*(6), 328-345. https://doi.org/10.1080/19393555.2012.747234

Razif, M., Miraja, B. A., Persada, S. F., Nadlifatin, R., Belgiawan, P. F., Redi, A. A. N. P., & Shu-Chiang, L. (2020). Investigating the role of environmental concern and the unified theory of acceptance and use of technology on working from home technologies adoption during COVID-19. *Entrepreneurship and Sustainability Issues*, *8*(1), 795-808. https://doi.org/10.9770/jesi.2020.8.1(53)

Reeves, A., Calic, D., & Delfabbro, P. (2021). “Get a red-hot poker and open up my eyes, it's so boring” 1: Employee perceptions of cybersecurity training. *Computers & Security*, *106*, 102281. https://doi.org/10.1016/j.cose.2021.102281

Reid, R., & Van Niekerk, J. (2014, August). From information security to cyber security cultures. In *2014 Information Security for South Africa* (pp. 1-7). IEEE. https://doi.org/10.1109/issa.2014.6950492

Reinfelder, L., Landwirth, R., & Benenson, Z. (2019, May). Security managers are not the enemy either. *In Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (pp. 1-7).* https://doi.org/10.1145/3290605.3300663

Reinheimer, B., Aldag, L., Mayer, P., Mossano, M., Duezguen, R., Lofthouse, B., ... & Volkamer, M. (2020). An investigation of phishing awareness and education over time: When and how to best remind users. In *Sixteenth Symposium on Usable Privacy and Security ({SOUPS} 2020)* (pp. 259-284). https://www.usenix.org/conference/soups2020/presentation/reinheimer

Renaud, K. (2011). Blaming noncompliance is too convenient: What really causes information breaches?. *IEEE Security & Privacy*, *10*(3), 57-63. https://doi.org/10.1109/msp.2011.157

Renaud, K., & Dupuis, M. (2019, September). Cyber security fear appeals: Unexpectedly complicated. In *Proceedings of the New Security Paradigms Workshop* (pp. 42-56). https://doi.org/10.1145/3368860.3368864

Renaud, K., & Flowerday, S. (2017). Contemplating human-centred security & privacy research: Suggesting future directions. *Journal of Information Security and Applications*, *34*, 76-81. https://doi.org/10.1016/j.jisa.2017.05.006

Renaud, K., & Zimmermann, V. (2018). Ethical guidelines for nudging in information security & privacy. *International Journal of Human-Computer Studies*, *120*, 22-35. https://doi.org/10.1016/j.ijhcs.2018.05.011

Reynolds, D. L., Garay, J. R., Deamond, S. L., Moran, M. K., Gold, W., & Styra, R. (2008). Understanding, compliance and psychological impact of the SARS quarantine experience. *Epidemiology & Infection, 136*(7), 997-1007. https://doi.org/10.1017/s0950268807009156

Rhee, H. S., Ryu, Y. U., & Kim, C. T. (2012). Unrealistic optimism on information security management. *Computers & Security*, *31*(2), 221-232. https://doi.org/10.1016/j.cose.2011.12.001

Rhee, H. S., Ryu, Y., & Kim, C. T. (2005). I am fine but you are not: Optimistic bias and illusion of control on information security. *ICIS 2005 Proceedings*, 32. https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1238&context=icis2005

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology*, *91*(1), 93-114. https://doi.org/10.1080/00223980.1975.9915803

Rogers, R. W., Deckner, C. W., & Mewborn, C. R. (1978). An expectancy-value theory approach to the long-term modification of smoking behavior. *Journal of Clinical Psychology*, *34*(2), 562-566. https://doi.org/10.1002/1097-4679(197804)34:2%3C562::aid-jclp2270340266%3E3.0.co;2-z

Ruhwanya, Z., & Ophoff, J. (2021, July). Critical analysis of information security culture definitions. In *International Symposium on Human Aspects of Information Security and Assurance* (pp. 353-365). Springer, Cham. https://doi.org/10.1007/978-3-030-57404-8_27

Ruighaver, A. B., Maynard, S. B., & Chang, S. (2007). Organisational security culture: Extending the end-user perspective. *Computers & Security*, *26*(1), 56-62. https://doi.org/10.1016/j.cose.2006.10.008

Ruiter, R. A., Abraham, C., & Kok, G. (2001). Scary warnings and rational precautions: A review of the psychology of fear appeals. *Psychology and Health*, *16*(6), 613-630. https://doi.org/10.1080/08870440108405863

Ruiter, R. A., Verplanken, B., De Cremer, D., & Kok, G. (2004). Danger and fear control in response to fear appeals: The role of need for cognition. *Basic and Applied Social Psychology*, *26*(1), 13-24. https://doi.org/10.1207/s15324834basp2601_2

Ruoti, S., Andersen, J., Monson, T., Zappala, D., & Seamons, K. (2018). A comparative usability study of key management in secure email. In *Fourteenth Symposium on Usable Privacy and Security ({SOUPS} 2018)* (pp. 375-394). https://www.usenix.org/conference/soups2018/presentation/ruoti

Saban, K. A., Rau, S., & Wood, C. A. (2021). SME executives' perceptions and the information security preparedness model. *Information & Computer Security, 29*(2), 263-282. https://doi.org/10.1108/ics-01-2020-0014

Sabillon, R. (2022). The Cybersecurity Awareness Training Model (CATRAM). In *Research Anthology on Advancements in Cybersecurity Education* (pp. 501-520). IGI Global. https://doi.org/10.4018/978-1-6684-3554-0.ch025

Saltzer, J. H., & Schroeder, M. D. (1975). The protection of information in computer systems. *Proceedings of the IEEE*, *63*(9), 1278-1308. https://doi.org/10.1109/proc.1975.9939

Sas, M., Hardyns, W., van Nunen, K., Reniers, G., & Ponnet, K. (2021). Measuring the security culture in organizations: a systematic overview of existing tools. *Security Journal*, *34*(2), 340-357. https://doi.org/10.1057/s41284-020-00228-4

Sasse, M. A., & Flechais, I. (2005). Usable security: Why do we need it? How do we get it?. O'Reilly. https://discovery.ucl.ac.uk/id/eprint/20345/

Sasse, M. A., & Rashid, A. (July, 2021). Human Factors Knowledge Area Version 1.0.1, CyBOK Version 1.0.1. Available at: https://www.cybok.org/knowledgebase1_1/ [Accessed 25 Jan. 2022]

Sasse, M. A., Brostoff, S., & Weirich, D. (2001). Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security. *BT Technology Journal*, *19*(3), 122-131. https://doi.org/10.1049/pbbt004e_ch15

Savage, I. (1993). Demographic influences on risk perceptions. *Risk Analysis*, *13*(4), 413-420. https://doi.org/10.1111/j.1539-6924.1993.tb00741.x

Sax, H., Uçkay, I., Richet, H., Allegranzi, B., & Pittet, D. (2007). Determinants of good adherence to hand hygiene among healthcare workers who have extensive exposure to hand hygiene campaigns. *Infection Control & Hospital Epidemiology*, *28*(11), 1267-1274. https://doi.org/10.1086/521663

Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a more representative definition of cyber security. *Journal of Digital Forensics, Security and Law*, *12*(2), 8. https://doi.org/10.15394/jdfsl.2017.1476

Scheier, M. F., & Carver, C. S. (1985). Optimism, coping, and health: assessment and implications of generalized outcome expectancies. *Health Psychology*, *4*(3), 219-247. https://doi.org/10.1037/0278-6133.4.3.219

Schlienger, T., & Teufel, S. (2003, September). Analyzing information security culture: increased trust by an appropriate information security culture. In *14th International Workshop on Database and Expert Systems Applications, 2003. Proceedings.* (pp. 405-409). IEEE. https://doi.org/10.1109/dexa.2003.1232055

Scolobig, A., De Marchi, B., & Borga, M. (2012). The missing link between flood risk awareness and preparedness: findings from case studies in an Alpine Region. *Natural Hazards*, *63*(2), 499-520. https://doi.org/10.1007/s11069-012-0161-1

Seawright, J., & Gerring, J. (2008). Case selection techniques in case study research: A menu of qualitative and quantitative options. *Political Research Quarterly*, *61*(2), 294-308. https://doi.org/10.1177/1065912907313077

Segreti, S. M., Melicher, W., Komanduri, S., Melicher, D., Shay, R., Ur, B., ... & Mazurek, M. L. (2017). Diversify to survive: Making passwords stronger with adaptive policies. In *Thirteenth Symposium on Usable Privacy and Security ({SOUPS} 2017)* (pp. 1-12). https://www.usenix.org/conference/soups2017/technical-sessions/presentation/segreti

Serafini, G., Parmigiani, B., Amerio, A., Aguglia, A., Sher, L., & Amore, M. (2020). The psychological impact of COVID-19 on the mental health in the general population. *QJM: An International Journal of Medicine, 113*(8), 531–537. https://doi.org/10.1093/qjmed/hcaa201

Sharot, T. (2011). The optimism bias. *Current Biology*, *21*(23), R941-R945. https://doi.org/10.1016/j.cub.2011.10.030

Shay, R., Komanduri, S., Durity, A. L., Huh, P., Mazurek, M. L., Segreti, S. M., ... & Cranor, L. F. (2016). Designing password policies for strength and usability. *ACM Transactions on Information and System Security (TISSEC)*, *18*(4), 1-34. https://doi.org/10.1145/2891411

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2010, April). Who falls for phish?: a demographic analysis of phishing susceptibility and effectiveness of interventions. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 373-382). ACM. https://doi.org/10.1145/1753326.1753383

Shepperd, J. A., Carroll, P., Grace, J., & Terry, M. (2002). Exploring the causes of comparative optimism. *Psychologica Belgica*, *42*(1/2), 65-98. https://doi.org/10.5334/pb.986

Shepperd, J. A., Klein, W. M., Waters, E. A., & Weinstein, N. D. (2013). Taking stock of unrealistic optimism. *Perspectives on Psychological Science*, *8*(4), 395-411. https://doi.org/10.1177/1745691613485247

Shepperd, J. A., Pogge, G., & Howell, J. L. (2017). Assessing the consequences of unrealistic optimism: Challenges and recommendations. *Consciousness and Cognition*, *50*, 69-78. https://doi.org/10.1016/j.concog.2016.07.004

Shepperd, J. A., Waters, E. A., Weinstein, N. D., & Klein, W. M. (2015). A primer on unrealistic optimism. *Current Directions in Psychological Science*, *24*(3), 232-237. https://doi.org/10.1177/0963721414568341n

Sherman, D. K., & Cohen, G. L. (2006). The psychology of self-defense: Self-affirmation theory. *Advances in Experimental Social Psychology*, *38*, 183-242. https://doi.org/10.1016/s0065-2601(06)38004-5

Sim, J., & Waterfield, J. (2019). Focus group methodology: some ethical challenges. *Quality & Quantity*, *53*(6), 3003-3022. https://doi.org/10.1007/s11135-019-00914-5

Sim, K., Chong, P. N., Chan, Y. H., & Soon, W. S. W. (2004). Severe Acute Respiratory Syndrome–Related Psychiatric and Posttraumatic Morbidities and Coping Responses in Medical Staff Within a Primary Health Care Setting in Singapore. *The Journal of Clinical Psychiatry, 65*(8), 1120-1127. https://doi.org/10.4088/jcp.v65n0815

Singh, S., Orwat, J., & Grossman, S. (2011). A protection motivation theory application to date rape education. *Psychology, Health & Medicine*, *16*(6), 727-735. https://doi.org/10.1080/13548506.2011.579983

Siponen, M., Pahnila, S., & Mahmood, M. A. (2010). Compliance with information security policies: An empirical investigation. *Computer, 43*(2), 64-71. https://doi.org/10.1109/mc.2010.35

Slovic, P. (1987). Perception of risk. *Science*, *236*(4799), 280-285. https://doi.org/10.1126/science.3563507

Slovic, P., Fischhoff, B., & Lichtenstein, S. (1980). Facts and fears: Understanding perceived risk. In *Societal risk assessment* (pp. 181-216). Springer, Boston, MA. https://doi.org/10.1007/978-1-4899-0445-4_9

Slupska, J. (2019). Safe at home: Towards a feminist critique of cybersecurity. *St Antony's International Review*, *15*(1), 83-100. doi: 10.1108/978-1-83982-848-520211049

Smith, R. A., Ferrara, M., & Witte, K. (2007). Social sides of health risks: Stigma and collective efficacy. *Health Communication*, *21*(1), 55-64. https://doi.org/10.1080/10410230701283389

Smithson, J. (2000). Using and analysing focus groups: limitations and possibilities. *International Journal of Social Research Methodology*, *3*(2), 103-119. https://doi.org/10.1080/136455700405172

Sommestad, T., Karlzén, H., & Hallberg, J. (2015). The sufficiency of the theory of planned behavior for explaining information security policy compliance. *Information & Computer Security*, *23*(2), 200-217. https://doi.org/10.1108/ics-04-2014-0025

Spinnewijn, J. (2015). Unemployed but optimistic: Optimal insurance design with biased beliefs. *Journal of the European Economic Association*, *13*(1), 130-167. https://doi.org/10.1111/jeea.12099

Stacey, P., Taylor, R., Olowosule, O., & Spanaki, K. (2021). Emotional reactions and coping responses of employees to a cyber-attack: A case study. *International Journal of Information Management*, *58*, 102298. https://doi.org/10.1016/j.ijinfomgt.2020.102298

Starman, A. B. (2013). The case study as a type of qualitative research. *Journal of Contemporary Educational Studies/Sodobna Pedagogika*, *64*(1). https://doi.org/10.7571/esjkyoiku.7.81

Stieger, S., & Göritz, A. S. (2006). Using instant messaging for Internet-based interviews. *CyberPsychology & Behavior*, *9*(5), 552-559. https://doi.org/10.1089/cpb.2006.9.552

Styra, R., Hawryluck, L., Robinson, S., Kasapinovic, S., Fones, C., & Gold, W. L. (2008). Impact on health care workers employed in high-risk areas during the Toronto SARS outbreak. *Journal of Psychosomatic Research, 64*(2), 177-183. https://doi.org/10.1016/j.jpsychores.2007.07.015

Tam, L., Glassman, M., & Vandenwauver, M. (2010). The psychology of password management: a tradeoff between security and convenience. *Behaviour & Information Technology*, *29*(3), 233-244. https://doi.org/10.1080/01449290903121386

Tan, K. L., Sia, J. K. M., & Tang, K. H. D. (2020). Examining students' behavior towards campus security preparedness exercise: The role of perceived risk within the theory of planned behavior. *Current Psychology*, 1-10. https://doi.org/10.1007/s12144-020-00951-6

Tang, J. S., & Feng, J. Y. (2018). Residents' disaster preparedness after the Meinong Taiwan earthquake: A test of protection motivation theory. *International Journal of Environmental Research and Public Health*, *15*(7), 1434. https://doi.org/10.3390/ijerph15071434

Tang, M., Li, M. G., & Zhang, T. (2016). The impacts of organizational culture on information security culture: a case study. *Information Technology and Management*, *17*(2), 179-186. https://doi.org/10.1007/s10799-015-0252-2

Tannenbaum, M. B., Hepler, J., Zimmerman, R. S., Saul, L., Jacobs, S., Wilson, K., & Albarracín, D. (2015). Appealing to fear: A meta-analysis of fear appeal effectiveness and theories. *Psychological Bulletin*, *141*(6), 1178. https://doi.org/10.1037/a0039729

Thrul, J., Belohlavek, A., Kaur, M., & Ramo, D. E. (2017). Conducting online focus groups on Facebook to inform health behavior change interventions: Two case studies and lessons learned. *Internet Interventions*, *9*, 106-111. https://doi.org/10.1016/j.invent.2017.07.005

Tilley, S. A. (2003). "Challenging" research practices: Turning a critical lens on the work of transcription. *Qualitative Inquiry*, *9*(5), 750-773. https://doi.org/10.1177/1077800403255296

Tischer, M., Durumeric, Z., Foster, S., Duan, S., Mori, A., Bursztein, E., & Bailey, M. (2016, May). Users really do plug in USB drives they find. In *2016 IEEE Symposium on Security and Privacy (SP)* (pp. 306-319). IEEE. https://doi.org/10.1109/sp.2016.26

Trumbo, C., Lueck, M., Marlatt, H., & Peek, L. (2011). The effect of proximity to Hurricanes Katrina and Rita on subsequent hurricane outlook and optimistic bias. *Risk Analysis: An International Journal*, *31*(12), 1907-1918. https://doi.org/10.1111/j.1539-6924.2011.01633.x

Tsai, H. Y. S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N. J., & Cotten, S. R. (2016). Understanding online safety behaviors: A protection motivation theory perspective. *Computers & Security*, *59*, 138-150. https://doi.org/10.1016/j.cose.2016.02.009

Tsakalidis, G., Vergidis, K., Madas, M., & Vlachopoulou, M. (2018). Cybersecurity threats: a proposed system for assessing threat severity. In *Proceedings of the the forth international conference on decision support system technology–ICDSST 2018*. https://doi.org/10.1007/978-3-030-18819-1_6

Tsohou, A., Karyda, M., & Kokolakis, S. (2015). Analyzing the role of cognitive and cultural biases in the internalization of information security policies: Recommendations for information security awareness programs. *Computers & Security*, *52*, 128-141. https://doi.org/10.1016/j.cose.2015.04.006

Tsohou, A., Karyda, M., Kokolakis, S., & Kiountouzis, E. (2015). Managing the introduction of information security awareness programmes in organisations. *European Journal of Information Systems*, *24*(1), 38-58. https://doi.org/10.1057/ejis.2013.27

Turland, J., Coventry, L., Jeske, D., Briggs, P., & van Moorsel, A. (2015, July). Nudging towards security: Developing an application for wireless network selection for android phones. In *Proceedings of the 2015 British HCI conference* (pp. 193-201). https://doi.org/10.1145/2783446.2783588

Tversky, A., & Kahneman, D. (1974). Judgment under uncertainty: Heuristics and biases. *Science*, *185*(4157), 1124-1131. https://doi.org/10.1126/science.185.4157.1124

Tversky, A., & Kahneman, D. (1981). *Judgments of and by representativeness* (No. TR-3). STANFORD UNIV CA DEPT OF PSYCHOLOGY. https://doi.org/10.21236/ada099502

Uchendu, B., Nurse, J. R., Bada, M., & Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. *Computers & Security*, *109*, 102387. https://doi.org/10.1016/j.cose.2021.102387

Unadkat, S., & Farquhar, M. (2020). Doctors' wellbeing: self-care during the covid-19 pandemic. *BMJ*, *368*. https://doi.org/10.1136/bmj.m1150

Ur, B., Bees, J., Segreti, S. M., Bauer, L., Christin, N., & Cranor, L. F. (2016, May). Do users' perceptions of password security match reality?. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (pp. 3748-3760). https://doi.org/10.1145/2858036.2858546

Van Audenhove, L., & Donders, K. (2019). Talking to people III: Expert interviews and elite interviews. In *The Palgrave handbook of methods for media policy research* (pp. 179-197). Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-030-16065-4_10

van Bavel, R., Rodríguez-Priego, N., Vila, J., & Briggs, P. (2019). Using protection motivation theory in the design of nudges to improve online security behavior. *International Journal of Human-Computer Studies*, *123*, 29-39. https://doi.org/10.1016/j.ijhcs.2018.11.003

Van Der Roest, D., Kleiner, K., & Kleiner, B. (2017). Self-Efficacy: The Biology Of Confidence. *Global Education Journal*, *2017*(1), 7-14. http://search.ebscohost.com/login.aspx?direct=true&profile=ehost&scope=site&authtype=crawler&jrnl=21523622&AN=134045952&h=Kc19ZhVGbG2HJ33E8JF4qjBP%2FFnU0%2BnrpKtdnx%2Bz6%2B96nLj9kMTLMmxMt5JfVc1FlchIDJH4xHQHT5itW0uPTw%3D%3D&crl=c

Van Middelkoop, M., Borgers, A., & Timmermans, H. (2003). Inducing heuristic principles of tourist choice of travel mode: A rule-based approach. *Journal of Travel Research*, *42*(1), 75-83. https://doi.org/10.1177/0047287503254116

Van Niekerk, J. F., & Von Solms, R. (2010). Information security culture: A management perspective. *Computers & Security*, *29*(4), 476-486. https://doi.org/10.1016/j.cose.2009.10.005

Van Schaik, P., Jansen, J., Onibokun, J., Camp, J., & Kusev, P. (2018). Security and privacy in online social networking: Risk perceptions and precautionary behaviour. *Computers in Human Behavior*, *78*, 283-297. https://doi.org/10.1016/j.chb.2017.10.007

Van Schaik, P., Jeske, D., Onibokun, J., Coventry, L., Jansen, J., & Kusev, P. (2017). Risk perceptions of cyber-security and precautionary behaviour. *Computers in Human Behavior*, *75*, 547-559. https://doi.org/10.1016/j.chb.2017.05.038

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & Management*, *49*(3-4), 190-198. https://doi.org/10.1016/j.im.2012.04.002

Vishwanath, A., Harrison, B., & Ng, Y. J. (2018). Suspicion, cognition, and automaticity model of phishing susceptibility. *Communication Research*, *45*(8), 1146-1166. https://doi.org/10.1177/0093650215627483

Vishwanath, A., Herath, T., Chen, R., Wang, J., & Rao, H. R. (2011). Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. *Decision Support Systems*, *51*(3), 576-586. https://doi.org/10.1016/j.dss.2011.03.002

Vogt, J. (2019). Human errors indicate problems in complex socio-technical systems–integrating not isolating natural and artificial intelligence is the answer. *Tagung der Fachgruppen AOW und ING, Braunschweig*. https://www.academia.edu/download/60616402/Vogt_Human_errors_are_symptoms_not_causes_of_socio-technical_problems_AI_must_be_integrated20190916-28539-a6yyr3.pdf

Volkamer, M., & Renaud, K. (2013). Mental models–general introduction and review of their application to human-centred security. In *Number Theory and Cryptography* (pp. 255-280). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-42001-6_18

von Solms, B., & von Solms, R. (2018). Cybersecurity and information security–what goes where?. *Information & Computer Security*, *26*(1), 2-9. https://doi.org/10.1108/ics-04-2017-0025

von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*, 97-102. https://doi.org/10.1016/j.cose.2013.04.004

Wakefield, J. (2020). Zoom boss apologises for security issues and promises fixes. *https://www.bbc.co.uk/news/technology-52133349*

Wakefield, M. A., Loken, B., & Hornik, R. C. (2010). Use of mass media campaigns to change health behaviour. *The Lancet*, *376*(9748), 1261-1271. https://doi.org/10.1016/s0140-6736(10)60809-4

Wang, B., Liu, Y., Qian, J., & Parker, S. K. (2021). Achieving effective remote working during the COVID-19 pandemic: A work design perspective. *Applied Psychology*, *70*(1), 16-59. https://doi.org/10.1111/apps.12290

Wang, J., Chen, R., Herath, T., & Rao, H. R. (2009). An exploration of the design features of phishing attacks. *Information Assurance, Security and Privacy Services*, *4*, 29. https://doi.org/10.1109/iaw.2007.381929

Wang, J., Li, Y., & Rao, H. R. (2017). Coping responses in phishing detection: an investigation of antecedents and consequences. *Information Systems Research*, *28*(2), 378-396. https://doi.org/10.1287/isre.2016.0680

Wang, L., & Alexander, C. A. (2021). Cyber security during the COVID-19 pandemic. *AIMS Electronics and Electrical Engineering*, *5*(2), 146-157. https://doi.org/10.3934/electreng.2021008

Ward, K., & Hawthorne, K. (1994). Do patients read health promotion posters in the waiting room? A study in one general practice. *Br J Gen Pract*, *44*(389), 583-585. https://bjgp.org/content/44/389/583.short

Warkentin, M., & Siponen, M. (2015). An enhanced fear appeal rhetorical framework: Leveraging threats to the human asset through sanctioning rhetoric. *MIS Quarterly*, *39*(1), 113-134. https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.677.1125&rep=rep1&type=pdf

Warkentin, M., Straub, D., & Malimage, K. (2012, June). Featured talk: Measuring secure behavior: A research commentary. In *Annual Symposium of Information Assurance & Secure Knowledge Management, Albany, NY.* http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.295.9566&rep=rep1&type=pdf

Waters, E. A., Klein, W. M., Moser, R. P., Yu, M., Waldron, W. R., McNeel, T. S., & Freedman, A. N. (2011). Correlates of unrealistic risk beliefs in a nationally representative sample. *Journal of Behavioral Medicine*, *34*(3), 225-235. https://link.springer.com/article/10.1007/s10865-010-9303-7

Weber, M. C., Schulenberg, S. E., & Lair, E. C. (2018). University employees' preparedness for natural hazards and incidents of mass violence: An application of the extended parallel process model. *International Journal of Disaster Risk Reduction*, *31*, 1082-1091. https://doi.org/10.1016/j.ijdrr.2018.03.032

Weil, T., & Murugesan, S. (2020). IT risk and resilience—Cybersecurity response to COVID-19. *IT Professional*, *22*(3), 4-10. https://doi.org/10.1109/mitp.2020.2988330

Weinstein, N. D. (1980). Unrealistic optimism about future life events. *Journal of Personality and Social Psychology*, *39*(5), 806-820. https://doi.org/10.1037/0022-3514.39.5.806

Weinstein, N. D. (1983). Reducing unrealistic optimism about illness susceptibility. *Health Psychology*, *2*(1), 11-20. https://doi.org/10.1037/0278-6133.2.1.11

Weinstein, N. D. (1989). Optimistic biases about personal risks. *Science*, *246*(4935), 1232-1234. https://doi.org/10.1126/science.2686031

Weinstein, N. D., & Klein, W. M. (1996). Unrealistic optimism: Present and future. *Journal of Social and Clinical Psychology*, *15*(1), 1-8. https://doi.org/10.1521/jscp.1996.15.1.1

Weirich, D., & Sasse, M. A. (2001, September). Pretty good persuasion: a first step towards effective password security in the real world. In *Proceedings of the 2001 Workshop on New Security Paradigms* (pp. 137-143). https://doi.org/10.1145/508171.508195

Whelan, C. (2017). Security networks and occupational culture: understanding culture within and between organisations. *Policing and Society*, *27*(2), 113-135. https://doi.org/10.1080/10439463.2015.1020804

Whitman, M. E. (2003). Enemy at the gate: threats to information security. *Communications of the ACM*, *46*(8), 91-95. https://doi.org/10.1145/859670.859675

WHO (World Health Organization). (2015, July 23). Summary table of SARS cases by country 1 November 2002 - 7 august 2003. http://www.who.int/csr/sars/country/2003_08_15/en/

WHO (World Health Organization). (2021, May 21). WHO Coronavirus Disease (COVID-19) Dashboard. https://covid19.who.int

Wikfeldt, E. (2016). Generalising from case studies. https://www.diva-portal.org/smash/record.jsf?pid=diva2%3A1051446&dswid=9821

Wiles, R. (2012). *What are qualitative research ethics?*. A&C Black. https://doi.org/10.5040/9781849666558

Wiley, A., McCormac, A., & Calic, D. (2020). More than the individual: Examining the relationship between culture and Information Security Awareness. *Computers & Security*, *88*, 101640. https://doi.org/10.1016/j.cose.2019.101640

Willems, C., & Meinel, C. (2012). Online assessment for hands-on cyber security training in a virtual lab. In *Global Engineering Education Conference (EDUCON), 2012 IEEE*(pp. 1-10). IEEE. https://doi.org/10.1109/educon.2012.6201149

Williams, C. M., Chaturvedi, R., & Chakravarthy, K. (2020). Cybersecurity risks in a pandemic. *Journal of Medical Internet Research*, *22*(9), e23692. https://doi.org/10.2196/23692

Williams, E. J., Hinds, J., & Joinson, A. N. (2018). Exploring susceptibility to phishing in the workplace. *International Journal of Human-Computer Studies*, *120*, 1-13. https://doi.org/10.1016/j.ijhcs.2018.06.004

Williams, K. C. (2012). Fear appeal theory. *Research in Business and Economics Journal*, *5*, 1. https://www.researchgate.net/profile/Kaylene-Williams/publication/265807800_Fear_Appeal_Theory/links/543857730cf2d6698bded352/Fear-Appeal-Theory

Williams, M., Nurse, J. R., & Creese, S. (2019a). (Smart) Watch Out! encouraging privacy-protective behaviour through interactive games. *International Journal of Human-Computer Studies*, *132*, 121-137. https://doi.org/10.1016/j.ijhcs.2019.07.012

Williams, M., Nurse, J. R., & Creese, S. (2019b). Smartwatch games: encouraging privacy-protective behaviour in a longitudinal study. *Computers in Human Behavior*, *99*, 38-54. https://doi.org/10.1016/j.chb.2019.04.026

Williams, M., Nurse, J. R., & Creese, S. (2016, August). The perfect storm: The privacy paradox and the Internet-of-Things. In *2016 11th International Conference on Availability, Reliability and Security (ARES)* (pp. 644-652). IEEE. https://doi.org/10.1109/ares.2016.25

Wired, C. (2018). *Cyber Security Risk: Perception vs. Reality in Corporate America*. [online] WIRED. Available at: https://www.wired.com/insights/2014/03/cyber-security-risk-perception-vs-reality-corporate-america/

Witte, K. (1992). Putting the fear back into fear appeals: The extended parallel process model. *Communications Monographs*, *59*(4), 329-349. https://doi.org/10.1080/03637759209376276

Witte, K. (1994). Fear control and danger control: A test of the extended parallel process model (EPPM). *Communications Monographs*, *61*(2), 113-134. https://doi.org/10.1080/03637759409376328

Witte, K. (1995). Generating effective risk messages: How scary should your risk communication be?. *Annals of the International Communication Association*, *18*(1), 229-254. https://doi.org/10.1080/23808985.1995.11678914

Witte, K. (1996). Fear as motivator, fear as inhibitor: Using the extended parallel process model to explain fear appeals successes and failures. In *Handbook of Communication and Emotion* (pp. 423-450). https://doi.org/10.1016/b978-012057770-5/50018-7

Witte, K., & Allen, M. (2000). A meta-analysis of fear appeals: Implications for effective public health campaigns. *Health Education & Behavior*, *27*(5), 591-615. https://doi.org/10.1177/109019810002700506

Wright, R. T., & Marett, K. (2010). The influence of experiential and dispositional factors in phishing: An empirical investigation of the deceived. *Journal of Management Information Systems*, *27*(1), 273-303. https://doi.org/10.2753/mis0742-1222270111

Xiao, Y., Becerik-Gerber, B., Lucas, G., & Roll, S. C. (2021). Impacts of working from home during COVID-19 pandemic on physical and mental well-being of office workstation users. *Journal of Occupational and Environmental Medicine*, *63*(3), 181-190. https://doi.org/10.1097/jom.0000000000002097

Xie, W., Fowler-Dawson, A., & Tvauri, A. (2019). Revealing the relationship between rational fatalism and the online privacy paradox. *Behaviour & Information Technology*, *38*(7), 742-759. https://doi.org/10.1080/0144929x.2018.1552717

Xu, F., & Warkentin, M. (2020). Integrating elaboration likelihood model and herd theory in information security message persuasiveness. *Computers & Security*, *98*, 102009. https://doi.org/10.1016/j.cose.2020.102009

Yamagishi, K. (1997). When a 12.86% mortality is more dangerous than 24.14%: Implications for risk communication. *Applied Cognitive Psychology: The Official Journal of the Society for Applied Research in Memory and Cognition*, *11*(6), 495-506. https://doi.org/10.1002/(sici)1099-0720(199712)11:6%3C495::aid-acp481%3E3.0.co;2-j

Yan, Y., Jacques-Tiura, A. J., Chen, X., Xie, N., Chen, J., Yang, N., ... & MacDonell, K. K. (2014). Application of the protection motivation theory in predicting cigarette smoking among adolescents in China. *Addictive Behaviors*, *39*(1), 181-188. https://doi.org/10.1016/j.addbeh.2013.09.027

Yin, R. K. (2009). *Case study research: Design and Methods* (Vol. 5). Sage. https://doi.org/10.3138/cjpe.30.1.108

Zacher, H., & Rudolph, C. W. (2021). Individual differences and changes in subjective wellbeing during the early stages of the COVID-19 pandemic. *American Psychologist*, *76*(1), 50–62. https://doi.org/10.1037/amp0000702

Zhang, S., Yu, L., Wakefield, R. L., & Leidner, D. E. (2016). Friend or foe: Cyberbullying in social network sites. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems*, *47*(1), 51-71. https://doi.org/10.1145/2894216.2894220

Zhang, X. A., & Borden, J. (2020). How to communicate cyber-risk? An examination of behavioral recommendations in cybersecurity crises. *Journal of Risk Research*, *23*(10), 1336-1352. https://doi.org/10.1080/13669877.2019.1646315

Zhang, Y., & Wildemuth, B. M. (2009). Unstructured interviews. *Applications of social research methods to questions in information and library science*, 222-231. https://www.researchgate.net/profile/Leonardo-Melo-

17/publication/262427146_Ciencias_sociales_bibliotecologia_y_ciencia_de_la_informacion_puntos_de_encuentro/links/56a7e1ec08aeded22e371b81/Ciencias-sociales-bibliotecologia-y-ciencia-de-la-informacion-puntos-de-encuentro.pdf

Zimmermann, V., & Renaud, K. (2019). Moving from a 'human-as-problem" to a 'human-as-solution" cybersecurity mindset. *International Journal of Human-Computer Studies*, *131*, 169-187. https://doi.org/10.1016/j.ijhcs.2019.05.005

Zurko, M. E., & Simon, R. T. (1996, September). User-centered security. In *Proceedings of the 1996 workshop on New security paradigms* (pp. 27-33). https://doi.org/10.1145/304851.304859

Zuwita, R. M., & Rahmatullah, B. (2021). Relationship between PMT appraisals and Security Practice: Analysis of prevention of insider threat in organization success factor. *Ilkogretim Online*, *20*(4). https://doi.org/10.1093/med-psych/9780190940164.003.0037