Gordon Institute of Business Science
University of Pretoria

The function of cyber-security awareness and training in shaping cyber-risk perceptions and resultant cyber behaviours

05092460

A research project submitted to the Gordon Institute of Business Science, University of Pretoria, in partial fulfilment of the requirements for the degree of Master of Business Administration.

01 November 2022

ABSTRACT

This study sought to explore cyber-risk perceptions that employees in South African financial services perceive that they as individuals and their respective organisations are exposed, the interventions implemented by organisations and the resultant cyber behaviours. The role-played cyber-security awareness and training intervention in shaping these cyber-risk perceptions and self-efficacy to mitigate such risks were explored in depth. The concept and influence of relatedness were then explored by comparing cyber behaviours within an individual cyber-risk perception context and organisational risk perceptions context. The research took a cross-sectional approach in 2022 and was conducted through a qualitative method, with data collected from 15 participants from nine organisations in the South African financial services industry. Collected data were analysed using thematic analysis, leveraging the Atlas.ti tool. Two of the four propositions were confirmed, whereas the other two were expanded to align with the findings from the study. The main implication of this study is for cyber-security managers to refine their cyber-security awareness and training programmes to approach the specific needs of each employee to keep them engaged and for them to keep benefiting from those programmes. There is a potential that well-crafted employee cyber-security training programmes could entice and attract more people into the cyber-security domain, which could help to close the growing skill shortage in this domain. This study contributes to the human cyber behaviour literature, particularly the protection motivation theory, by distinguishing between individual and organisational cyber-risk. Earlier studies in this domain focused on these contexts separately and not comparatively in a single study similar to this research.

Keywords

cyber-risk; cybercrime; organisational interventions; cyber-security; cyber behaviour

DECLARATION

I declare that this research project is my own work. It is submitted in partial fulfilment of the requirements for the degree of Master of Business Administration at the Gordon Institute of Business Science, University of Pretoria. It has not been submitted before for any degree or examination in any other University. I further declare that I have obtained the necessary authorisation and consent to carry out this research.

Naomi Mahlatje
01 November 2022

CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1: INTRODUCTION TO RESEARCH PROBLEM

1.1 Introduction and problem definition

Business leaders today cannot afford the lack of a well thought, proactive and holistic strategy for cyber-risks encountered by businesses, employees, customers, and government (Segal, 2022). Cyber-risks are no longer departmental but enterprise-wide, with potential systemic influences for organisations, shareholders, and broader stakeholders. These include individuals that directly or indirectly depend on services from such organisations (Choudhury, 2020; Segal, 2022). Cyber incidents affecting banks could have a systemic economic influence, with Eisenbach et al. (2021) presenting that as much as 31% of economic activities could be brought to a standstill if five of the US' most active banks were compromised. While the availability of data breaches a is a challenge to the quantification of cyber-risks, some researchers presented that a cyber breach can consume as much as 1.09% of the organisation's shareholder value (Kamiya et al., 2021; Tosun, 2021).

Regulatory bodies have enacted compliance requirements for organisations to comply to, reducing their cyber-risk (Mutune, 2020). In South Africa, for example, *Protection of Personal Information Act 4 of 2013* (POPIA), which came into effect on 1 July 2021, was the government's intervention to ensure that organisations safeguard the personal identifiable information they collect and process (South African Government, 2013). It is; however, contended that compliance to such regulatory requirements only provide minimal levels of cybersecurity and have not proven to be sufficient to remediate cyber-risks as an organisation can be compliant yet be subjected to cybercrime if the controls are not implemented effectively (Taylor, 2018). This is further attested by lack of correlation established between compliance-based cyber audits and the probability of cyber incidents and breaches (Slapničar et al., 2022).

Cybercrime costs individuals and businesses across the globe billions of dollars annually and these numbers are not showing any signs of slowing down (Bendovschi, 2015; Clough, 2011; Kshetri, 2019); Monteith et al., 2021). The 2021 IBM Cost of Data Breach Report reported a 9.8% year-on-year increase in the cost of data breach to $4.2 million,

with a significant portion (38%) of the cost attributed to losing business arising from the breach (IBM Report: *Cost of a Data Breach Hits Record High during Pandemic,* 2021) In the US, for example, The Federal Bureau of Investigation's 2021 *annual internet crime report* presented an annual loss, exceeding $6.9 billion—a 7% increase from the prior year (Federal Bureau of Investigation, 2021). The risk of cybercrime is not only on an upward slope for organisations but for individuals in their personal capacity. The South African Banking Risk Information Centre (SABRIC) reported a 33% increase in digital banking fraud in 2020 ("SABRIC Annual Crime Statistics 2020," 2020).

The COVID-19 pandemic has fuelled the need for online services from social, and corporate collaboration, shopping, and banking, to name a few (Baig et al., n.d.). At a global level, it was reported in 2021 that 197 million emails and 69 million instant messages were sent every minute, while almost $100 million was spent online every hour (Jenik, 2021). Compared to pre-COVID, the money spent online increased by about 60% (Desjardins, 2019). Similar patterns were reported in South Africa, with one of the local banks reporting a 55% and 42% increase in online spend on their platforms for 2020 and 2021, respectively (Partner, 2021). Customer demands, employee productivity and endorsing competitive advantage are driving forces to the ever-increasing adoption of online digital platforms and Internet-based services ("Digital Commerce Acceleration," 2021). Digital communications, such as instant messaging, email and video collaboration devices, have also become a norm and have gained even further adoption with the COVID-19 pandemic (Baig et al., n.d.).

With high levels of transactions of communications online, cybercrime is also ever-increasing, and the indication is this will continue to be the case as cybercriminals keep pursuing to have a 'piece of the pie' (Cheung et al., 2021). Cybercriminals may target individuals, business organisations, and even state-owned organisations (Ablon, 2018). While various authors may have names for distinct types of cyber criminals based on their motivation, such as hackers, cyberterrorists, hacktivists, state-sponsored (Ablon, 2018). The term *cybercriminal* was used in this study as it was more encompassing.

Most cybercrimes are motivated by financial gains (Loughran, 2020). The top five cybersecurity threats facing organisations today are 1) social engineering and phishing, 2)

ransomware, 3) Distributed-Denial-of-Service attacks, 4) compromise of third-party software, and 5) cloud computing vulnerabilities (Lauver, 2022). Social engineering tactics are the most prevalent and successful attacks. It was recorded that 32% of successful cyberattacks in 2020 involved a social engineering tactic called phishing (Deloitte, 2020).

In the simplest form of cybercrime, cybercriminals may steal data to sell it to willing buyers on the dark web (Ablon, 2018). Other examples of financially motivated cybercrimes include cases where cybercriminals may hijack or mimic an identity of a trusted party and use it to extort money from unsuspecting people connected to this person or perform financial transactions using that individual's information (Ablon, 2018). Cybercriminals can intercept email communications and alter the original emails; for example, send their banking details for payments of business transactions to be made into their accounts (Sher-Lun & Nicoll, 2020). In more sophisticated attacks, cybercriminals can compromise individual or organisation data and systems and them to ransom by encrypting them and demanding that money be paid to restore the owner's access to the data and system or threatening to make such data public (O'Kane et al., 2018).

Besides the financial gains as a motivation for cybercriminals, it is not uncommon for cybercriminals to have other motives, such as political and espionage (Bronk, 2015; Härting et al., 2022). From the political perspective, an example is during the height of Russia and Ukraine unrest in 2022, countries such as UK and the US anticipated their critical infrastructures to be targeted by Russia-sponsored cyberattacks and issued formal warnings to their stakeholders to prepare for these attacks (Quallo-Wright, 2022; Ikeda, 2022). Another notable example of politically motivated attacks was related to the Black Life Matters movement, were infrastructure related to the movement was targeted with distributed-denial-of-service attacks, which were believed to be efforts to silence the movement (Brewster, 2020).

Cyber espionage is a type of cybercrime often conducted by state-sponsored syndicates; they are executed to obtain intelligence to advance the interests of the perpetrator or their client at the victim's expense (Ablon, 2018; Deibert & Rohozinski, 2009). Cyber espionage cyberattacks against organisations may include theft of intellectual property, such as trade secrets, confidential differentiating strategies, research, and developments information

before publicly available, therefore, compromising the victim organisation's competitive advantage (Bressler & Bressler, 2014). In 2010, Google suffered espionage when its proprietary source code, which was part of its intellectual property, was stolen (Finkle, 2010). Economically motivated cyber espionage attacks are also common in the trading realm, where having access to trading information at advantageous times would enable the cybercriminals or their respective clients to have an unfair advantage in the market (Ablon, 2018).

Social engineering is the method of conducting cybercrime where attackers use unsuspecting people to conduct their malicious actions (Salahdine & Kaabouch, 2019). Phishing is the social engineering attack where cybercriminals make use of emails to conduct malicious activities, such as soliciting confidential information from the victim, tricking the victim into performing fraudulent transactions under the guise of a known and trusted identity or infecting the device and network from which the user is connected or even download malware and infect the victim's device and network to which there are connected (Pienta et al., 2020).

These cyberattacks rely on human psychology and invoke emotions, such as fear and empathy, to convince the victim to conduct actions that act as the last mile for the cybercriminal's objectives (Pienta et al., 2020). Using social engineering tactics in cybercrime was evident in the FBI's Internet crime report where financial losses associated with email-based cybercrime amounted to almost 35% of the total reported financial losses (Federal Bureau of Investigation, 2021). While politically motivated cybercrime should not be ignored, most cybercriminals remain financially motivated (Loughran, 2020).

Employees are the highest threat encountering organisations, an observation often contended to be associated with high risk, attributed to human vulnerability to social engineering attacks (Lee. 2021; Workman, 2007). Social engineering-based cyberattack methods can be thwarted through constant alertness and practising cyber protective behaviours (Pienta et al., 2020). Human vulnerabilities call for organisations to have holistic cybersecurity programmes, surpassing deployments of various technological solutions. Programmes that include more than firewalls, identity, and access management solutions, endpoint and device security, and email security solutions with advanced

security technology solutions that use artificial intelligence and machine learning to detect even unknown attacks based on user or device behaviour (NIST, 2018; Wiafe et al., 2020), but include strategies to leverage people as the last layer of protection are what businesses require today to reduce their cyber-risk (Salahdine & Kaabouch, 2019).

1.2 Purpose and research problem

1.2.1 Business problem

The main research question is:

How can organisational leaders and cybersecurity professionals leverage individual cyber-risk perceptions in their cybersecurity awareness and training programmes aimed at shaping employee protective cyber behaviours?

Given that most cybercrimes involve social engineering tactics, the function of employee cyber behaviour in improving the resilience of organisations from cybercrime cannot be overestimated (Deloitte, 2020). The significance of the role played by humans in the cybersecurity of the sociotechnical ecosystem has increased interest in the study of human behaviour in the cybersecurity domain over the past few decades (Workman, 2007; Pienta et al., 2020). Business leaders and cybersecurity professionals need to understand how they can positively influence their employees' cyber behaviours to help them reduce their organisational cyber-risk exposure (Ogbanufe et al., 2021).

This study was conducted in the South African financial services industry. The financial services industry was selected for this study as it remains the most lucrative market for cybercriminals, and creating a cybersecurity-conscious culture in this sector will be beneficial to this important sector (Kshetri, 2019). Attributable to the central function of financial service organisations in a market, they have the potential to cause systemic influence when struck by cybercrime (Kshetri, 2019; Eisenbach et al., 2021). According to the 2021 Internet Crime Report, South Africa was the fifth country globally to suffer from cybercrime, after Canada. India, Australia, and France, strongly indicative of the severity cyber-risks in this country (Federal Bureau of Investigation, 2021)

1.2.2 Academic problem

The criticality of the role played by humans in cybersecurity has spiked interest in research in this space (Mou et al., 2022; Sommestad et al., 2015). Existing behaviour-based theories, such as protection motivation theory (PMT), have been applied in the cybersecurity domain to understand the relationship between motivation and behaviour (Liang & Xue, 2010; Menard et al., 2017; Carpenter et al., 2019; Donalds & Osei-Bryson, 2020; Gillam & Foster, 2020; Mou et al., 2022). PMT theory emanates from the health domain where the perceived risk was the subject's own health or life (Wang et al., 2019), and on the same premise, the applicability of the PMT model in the cybersecurity space has not been without criticism from some learners, with critics pointing the lack of direct danger in cybersecurity and, therefore, questioning the relevance and accuracy of the model in this domain (Vishwanath et al., 2020).

This research aimed to respond to a call for a study, clarifying cyber-risk from the individual and the organisational perspective, such as cross-domain cyber-risk, as little research has been conducted on this (Pienta et al., 2020). Most cyber-risk studies were from siloed contexts, i.e., from either an individual perspective (Mishna et al., 2009; Chen & Zahedi, 2016) or an organisational perspective (Burns et al., 2017; Donalds & Osei-Bryson, 2020; Gillam & Foster, 2020). The study adds to the body of literature on cyber-risk by creating an understanding of how organisational interventions, such as cybersecurity awareness training, can instil protective cyber behaviours among employees in their workplace, leveraging the personal closeness that employees have in their perceived individual cyber-risks

1.3 Conclusion

This chapter outlined the research problem, objective, and scope of the study. In the next chapter, an in-depth literature review from peer-reviewed articles was conducted to obtain a further understanding of the extend of prior research conducted and emphasise divergences in the literature for this topic. Chapter 3 then outlined the theoretical propositions; the research design and methodology are described in Chapter 4, while Chapter 5 and 6 concerned the data analysis and discussion, respectively. Finally, in

Chapter 7, the conclusions are drawn, business and theoretical implications are presented, and finally, the limitations of this study and the suggestions for future studies were then outlined.

CHAPTER 2: LITERATURE REVIEW

2.1 Introduction

This chapter summarised the outcome of the review of existing literature on the current topic. Cyber-risk, with terms closely related to cyber-risks, such as cybersecurity and cybercrime, were unravelled and defined first as this definition was the underlying base for the rest of this research. Types of cyber-risks were explored, and then various risk mitigation mechanisms adopted by organisations were outlined according to the literature findings. Cybersecurity awareness and training and technical security measures applied as organisational cyber-risk countermeasures were explored. Finally, two main risk theories, namely risk compensation theory and protection of motivation theory were explored in detail.

2.2 Cyber-risks

Cyber-risks include all unintentional impact that may cause compromise of confidentiality, integrity, and availability of information resources and or enabling technology and services, which can cause economic loss owing to operational disruptions, regulatory fines, response efforts and time, customer loss owing to reputational damage (Aldasoro et al., 2022). Strupczewski (2021) coined a more comprehensive definition encompassing the 1) source of the risk, 2) object at risk and 3) influence of cyber-risk from the organisation's perspective, and they comment: “Cyber-risk is an operational risk associated with the performance of activities in the cyberspace, threatening information assets, ICT resources and technological assets, which may cause material damage to tangible and intangible assets of an organisation, business interruption or reputational harm. The term ’cyber-risk’ also includes physical threats to the ICT resources within an organisation” (Strupczewski, 2021, p6). From the individual perspective, cyber-risks include additional social-oriented influences, such as cyber bullying, cyber stalking, and online embarrassment (Lievens, 2014; Shahria et al., 2020).

2.2.1 Related terms

Two terms that closely relate to cyber-risk and are sometimes used interchangeably are

information security and *cybersecurity*. Information security concerns protecting confidentiality, integrity and availability of the information assets owned by the organisation or individuals. Cybersecurity refers to the protection of cyber-present information and the protection of people and organisations against other hazards, such as cyber bullying, physical security, and brand damage (Shahria et al., 2020; Caldarulo et al., 2022). In cybersecurity, humans and organisations are not only compromised to obtain access to their resources but could be compromised to have them unknowingly participate in other cyberattacks, the effects of which can be even more damaging (von Solms & van Niekerk, 2013). Cybersecurity can be described as "… the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organisation and user's assets" (von Solms & van Niekerk, 2013, p97).

2.2.2 Sources of cyber-risks

Cyber-risk could emanate from either intentional cybercrime perpetrated by cybercriminals or from accidental incidents where actors such as internal employees and trusted third parties could pose the threat of these cyber-risks (Chng et al., 2022; Johnston et al., 2019; Warkentin et al., 2016). External cyber attackers varied in motivation, experience and access to resources, with some individuals acting in their own capacity and others as part of syndicate groups with various motivations; for example, nation states attackers are typically the most resourced and most skilled cyber attackers who are often driven by political and financial gain motivation while of the other end of the spectrum are novices or script kiddies who are less experienced and driven by curiosity (Chng et al., 2022). Petty thieves are cyber criminals financially driven that target organizations and individuals (Chng et al., 2022).

Internal people could either maliciously compromise the organisation, or unknowingly function as an enabler to external threats, for example, by clicking on a malicious link and enabling the compromise of their login credentials, infection of their device, or even the entire network (Pienta et al., 2020). Many researchers have identified employees, including contractors with internal system access, as the worst cyber-risk threats in the cybersecurity value chain (Aloul, 2012; Provos et al., 2009; Warkentin et al., 2012), while

some argued that humans are last layer of defence when the preventative technology measures had failed (Zimmermann & Renaud, 2019). Other researchers contend that while external attackers are a threat to cyber-risk, from the organisations' perspective, insiders present the greatest threat to cyber-risk, whether they act maliciously or erroneously (Li et al., 2019; Pienta et al., 2020; Song & Moon, 2020; Warkentin et al., 2016).

2.2.3 Organisational cyber-risks and evolution thereof

Introduction of end-user computing in the late 1980's and the proliferation of internet-enabled services and internet users have made the cyber space an attractive place to commit crime (Lee, 2021). Cybercrime was on the rise, but the complexity and sophistication of these crimes was also increasing faster than how systems and people could fight against them (Aldaroso et al., 2022; Dawson & Thomson, 2018; Gillam & Foster, 2020). The availability of advancing technology, such as artificial intelligence, was not only used by businesses to better their value propositions, but cybercriminals were also leveraging the same technologies to commit cybercrime (Almarhabi et al., 2022). The cyber landscape, the ground on which cybercrime was conducted, was also increasing through a proliferation of internet-connected users and devices, including devices not traditionally known to have or designed to be connected to the internet, such as fridges, cameras, and TVs; this concept is known as the Internet of Things (IoT) (Lee, 2021).

Adoption of the remote workforce was accelerated during the COVID-19 pandemic and appeared to be a new way of working for several organisations, meaning that most people no longer worked from their offices, and more people were also working from their personal devices (*bring your own device*), adding more complexities to the landscape that cybersecurity professionals needed to protect from cybercrime and erroneous cyber incidents (Almarhabi et al., 2022; Curran, 2020).

Another trend noted to have gained momentum was third-party or supply chain cyber-risk (Kumar et al., 2022). It has become common practice to see businesses outsourcing some of their business processes, use 3rd party software solutions to run their business processes or leverage IT infrastructure running from cloud providers to allow for cost

optimisation and business agility and competitiveness (Asatiani et al., 2019; Gambal et al., 2022; Hon & Millard, 2018). While all these external parties extended the cyber-risk that businesses, individuals and even government states got exposed to, there was also an increased risk of systemic influence when these providers were compromised (Eisenbach et al., 2021). A recent example of a third-party cyber breach that exposed corporate client's sensitive information in South African financial services includes African Bank in 2021, and from the telecommunication perspective, Vodacom suffered a similar third-party breach in 2022 (Labuschagne, 2022; Monzon, 2021).

Organisations have, over the years, improved their technical security posture. This presented the main reason cybercriminals have shifted their focus to compromising human vulnerabilities to get a foothold into a network and other resources of their interest, such as sensitive information (Aloul, 2012). Financial services made for attractive targets for cybercrime not only because they managed money, but the information they posessed could also be easily converted to money (Aldaroso et al., 2022). In other geographic areas, such as the US, while financial services were attacked the most, they lost less money from these attacks compared to other industries, a position attributed to technology investments that financial services implemented in this area (Aldasoro et al., 2022). No comparable evidence was found for the South African market.

2.2.4 Cyber-risk in the financial services industry

Financial services were among the sectors targeted by cybercrime, and this could be contended that despite being one sector focusing on cybersecurity from the early days of the boom of the Internet. Financial services industry organisations remained a lucrative market for cyber criminals (Eisenbach et al., 2021; Kshetri, 2019; Lee, 2021. Given the function of financial services in any economy and the global economy, the compromise of their infrastructure, systems, and data could have a ripple effect, affecting relying businesses and individuals (Eisenbach et al., 2021, Burton et al., 2022). The cybersecurity drive by financial services organisations should, therefore, not only be observed from the operational and financial influence perspectives but from the influence of the customer that entrusted organisations with their sensitive, personal information. If this personal and financial data got into the wrong hands, it could be devastating to the customers (Reveron

& Savage, 2020).

2.2.5 Individual cyber-risks

Individuals faced cyber-risks in their personal capacities and as employees (Cain et al., 2018). In personal capacity, individual cyber-risks included those risks that they inherited in their capacities as customers or service recipients, such as loss of service (availability), theft of personal information (confidentiality) and negative fiscal influence (integrity) (Pienta et al., 2020). Individuals also faced socially oriented cyber-risks, such as cyberstalking, online harassment and cyberbullying (Shahria et al., 2020; Caldarulo et al., 2022).

Identity theft or loss of login credentials are cyber-risks were said to have a possible downstream impact, such as fraud or account hijacking (Lai et al., 2012). Social media account hijacking is an example of compromised login credentials where the cybercriminal can assume the medial social identity of an individual and post malicious content or solicit money from people using this stolen social identity (Irshad & Soomro, 2018; Shahria et al., 2020). This cyber-risk presented individual reputational damage risk that can harm social and professional worlds where jobs could be lost (Irshad & Soomro, 2018). Identity theft could also cause economic loss to the victim through the hijacking of financial services or making fraudulent purchases in the victim's name (Lai et al., 2012; van de Weijer et al., 2018).

Social engineering referred to tactics cybercriminals leverage to exploit human vulnerabilities (Vishwanath et al., 2016). Individuals were known to be subjected to social engineering cyber-attacks in their personal capacity and as employees (Strupczewski, 2021). One example of social engineering mostly studied is phishing (Alsharnouby et al., 2015; Vishwanath et al., 2016; Pienta et al., 2018). While data availability is scarce for personal cyber-attacks, phishing is cited as one of the commonly used methods of cyber-attacks (Aldasoro et al., 2022). Most successful organisational cyber-attacks included phishing somewhere in the attack chain (Kamiya et al., 2021). Phishing, therefore, presented the costliest cyber incidents (Aldasoro et al., 2022). Other types of social engineering tactics leveraged by cybercriminals, included leveraging phone calls (vishing)

and SMS (smishing) (Mishra & Soni, 2020).

Phishing emails vary in sophistication and approach (Pienta et al., 2018). Less sophisticated, spray and pray phishing approaches require fewer preparations and target a large population, hoping a small percentage of those that receive the phishing email may take the bait (O'Leary, 2019). Spear phishing and whaling were more sophisticated and targeted approaches where the cybercriminals study and analyse their target to increase their chances of succeeding when they launch the target (Pienta et al., 2020). Not everyone had the same levels of cyber-risk; some people make more attractive targets to cyber criminals than others. For example, older generations, and untrained young people are examples of those identified to have cyber-risks, higher than others (Mishna et al., 2009; van Schaik et al., 2017).

Social media was another arsenal with a wealth of information and reach for cybercriminals. Social media can profile victims for sophisticated and targeted cyber-attacks (Irshad & Soomro, 2018; Shahria et al., 2020). These platforms can also propagate malware from known and trusted forums to unsuspecting users (Labuschagne et al., 2012). More prevalent in younger people, social media can also expose people to cyber bullying, cyber stalking, and online harassment (Karklins & Dalton, 2012; Dredge et al., 2014; Musetti et al., 2022).

From the employee perspective, the influence of consequences of cyber incidents had varying types of influence depending on the type of role. For general employees at the lower part of the organisational hierarchy, the influence of a cyber incident might only include loss of productivity, for example, if their device was compromised or their work data was lost (Ogbanufe et al., 2021). Top management might encounter severe personal consequences such as job losses and even jail sentences (Ogbanufe et al., 2021; Gale et al., 2022; *(South African Government, 2013).* It could, therefore, be deduced that non-cybersecurity employees have a lower individual cyber-risk compared to senior members of the organisation and cybersecurity employees (Ogbanufe et al., 2021).

Personal influence from cybersecurity compromise incidents could range from privacy violation, economic loss, and even physical harm to death (Aldasoro et al., 2022).

Organisations that formed part of the nation's critical infrastructure, such as transport, health services, utilities, and telecommunications, could lead to life or death (Stine et al., 2017). The 2020 incident in Germany, where a woman died due to delayed services caused by the hospital's system being compromised, is an example of loss of life due to a cyber incident (Eddy & Perlroth, 2020). Cyber-risk to nations' critical infrastructure, including financial services, could be considered a matter of national security (Reveron & Savage, 2020).

2.3 Cyber-risk countermeasures

2.3.1 Technical measures

Organisations have focused on technical security control measures to counter cyber-risks (Dawson & Thomson, 2018). Technical countermeasures include firewalls, malware protection, authenticators, and encryption could protect individuals and organisations in cyber space against cybercrime. (Pienta et al., 2020). These technical countermeasures to cybercrime have positive advances through use of artificial intelligence such as machine learning; for example, malware protection technologies have evolved from simple signature-based prevention where malware infection could only be prevented if the malware in question is already known to the malware protection technology (Li, 2018; Zeadally et al., 2020).

Today malware protection technologies aim not only to prevent but can also heuristically detect that a device is under malware attack, and based on the set configured policies, the device could be automatically isolated from the network, force a shutdown until rebooted in a safe mode to protect any additional harm to the device and the network it is connected to (Li, 2018). This evolution is an acknowledgement that it is no longer a matter of whether a cyberattack will hit but when and organisations are struck, therefore, they should be gearing up for the inevitable (Antonescu & Birău, 2015).

Despite improving technical countermeasures, cybercrime remains persistent, suggesting that as good guys become better, the bad ones outpace the good ones in their becoming *more bad* and faster (Dawson & Thomson, 2018; Jalali et al., 2019). These technological advancements are two-edged sword as cybercrime perpetrators leverage the same to

further their criminal activities (Wang et al., 2021).

2.3.2 Cybersecurity awareness and training

Cybersecurity programmes in organisations have traditionally been focused on technical controls to fortify the network perimeter and infrastructure, including end-user devices, and cybercriminals have shifted their focus to exploiting human vulnerabilities. Internal people, such as IT Professionals, cybersecurity Professionals; general staff members, management teams and executive, forms an important part of the sociotechnical system and may be threats to this system (Aloul, 2012; Öğütçü et al., 2016; Witsenboer et al., 2022; Zimmermann & Renaud, 2019).

While it was understood that there may be malicious internal threats, it was also contended that malicious insiders represent a small portion of the internal userbase, and most of the internal users only act as a threat to the organisation owing to error or lack of knowledge despite these non-malicious actions by insiders contributing to the highest proportion of cyber incidents (Zimmermann & Renaud, 2019). To effectively mitigate cyber-risks, therefore, cybersecurity programmes needed to focus on building awareness and training end-users on cybersecurity, including cyber-risks (Jalali et al., 2019).

Cybersecurity awareness and training is a non-technical cyber-risk countermeasure employed by organisations to augment the technical measures and bolster resilience from the human aspect of the cybersecurity sociotechnical system (Pollini et al., 2021). Despite the advancing technical countermeasures implemented by organisations to safeguard their data and information systems, it was contended that the next weakest link in the sociotechnical eco-system targeted by cyber criminals was internal people (Abraham & Chengalur-Smith, 2010; Lee, 2021).

Awareness of the cyber-risk landscape and organisational security policies with training on actions and behaviours required to attend to such risks to reduce human error and intentional misuse of information systems, including the insider threat encountered by organisations (D'Arcy et al., 2009; Siponen, 2000). The employee base comprised a collection of people with vast levels of cyber awareness, which made the job of those responsible for designing cybersecurity awareness to be challenging (Siponen, 2000).

Despite being informed and aware of cyber-risk and the recommended actions to counter such risks, it was common for employees to take actions and behaviours known to be risky (Hadlington, 2018). Factors such as lack of personal closeness to the perceived cyber-risks and perceived higher costs concerning time and effort were among those identified and empirically assessed in certain contexts as contributors to risky cyber actions and behaviours (Mou et al., 2022).

2.4 Cyber behaviours

There was a wide range of practices that end-users can adopt to counter the inherent cyber-risk in their employee and personal capacities. Different terms were used to describe these cyber-risk reduction practices, namely: cyber hygiene, protective behaviour, and protection behaviour. Cyber hygiene was originally adopted from the public health domain as a broad set of cleanliness practices for protection against germs and diseases (Vishwanath et al., 2020). Cyber hygiene refers to the cybersecurity behaviours that online users should practice to safeguard the confidentiality, availability and integrity of their personal and organisational information and digital assets applied in the cybersecurity domain (Vishwanath et al., 2020). Cyber protective and cyber protection behaviour are adopted from Threat Motivation Theory (PMT). The term *protective cyber behaviour* was used in this study for consistency.

Hinging on the common belief that humans were the weakest link in cybersecurity (Abraham & Chengalur-Smith, 2010; Aloul, 2012; Zimmermann & Renaud, 2019; Lee. 2021), it was commonly believed that human vulnerabilities could be reduced when users practice protective cyber behaviours (van Bavel, Rodríguez-Priego, et al., 2019). The definition of cyber protective behaviours was not standardised with various researchers, professionals, and organisations having their unique interpretation of what protective cyber behaviours entailed. For example, one study presented thirteen cyber protective actions to define protective cyber behaviours Cain et al., 2018), another listed thirty-two cyber protective actions (Vishwanath et al., 2020), yet from another one listed fifteen actions (Witsenboer et al., 2022).

Common themes noted from these protective cyber behaviour studies included password

complexity, password changes, use of multifactor authentication, being cautious of phishing emails, reporting suspicious activities, backing up important data, using malware protection, checking the security of websites, tightening privacy settings on social media, no name a few. Vishwanath et al. (2020) proposed a conceptual model that categories these actions into five domains, such as 1) storage and device hygiene, 2) transmission hygiene, 3) social media hygiene, 4) authentication and credential hygiene, and 5) email and messaging hygiene (Vishwanath et al., 2020).

These protective cyber actions or behaviours have varied levels of technicality and effort; for example, it is a more technically involved to install and configure a firewall than to confirm the email sender's address (Vishwanath et al., 2020). The technicality of protective cyber behaviours has direct implications for end-user's knowledge and skills to carry those actions out. In the organisational setting, technical protective cyber behaviours, such as malware protection, software updates and applying security configuration settings, are centrally performed by the organisation.

At the same time, end-users need to holistically fend for themselves in the home settings absent the IT staff making them more vulnerable to cybercrime that targets system vulnerabilities than organisations (Vishwanath et al., 2020). The remainder of this section delved deeper into some commonly studied theories in human behaviour within cybersecurity to understand what shapes people's intention and practice of protective cyber behaviours.

2.4.1 Risk compensation model

The risk compensation model posits that human risk-taking behaviour is an act of balancing perceived costs and benefits in non-monetary terms (Van Schaik et al., 2017). Adams defined the risk compensation model in 1988 as a basis of continuous human risk-taking behaviour. According to this theory, cost considerations could include the time and effort of conducting actions, while the benefit may be the convenience that the person gets as their perceived reward for their action. Each individual and, therefore, organisations had a unique calibration of this sense of balance in cost and benefit (Van Schaik et al., 2017).

One of the important contributors to risk perception formulation is information availability (Gillam & Foster, 2020; Van Schaik et al., 2017). Perhaps when the person did not know that a certain action or lack thereof would increase or decrease their risk exposure, they would not review such action considering this risk. While information availability relates to the cognitive component of risk perception, another factor relates to how the emotions and emotions associated with the element imposing the risk are called the affect heuristic (Van Schaik et al., 2017).

Affect heuristics refer to a positive emotion from an action that causes risk exposure (Van Schaik et al., 2017). These positive emotions played a role in the benefit estimation part of the risk perception formulation process and, therefore, influence the decision someone would take in dealing with such risk. An example of smoking, outside of the cybersecurity domain, had a more emphasised illustration of affect heuristics in that while people might have information about the potential harm caused by smoking, the gratification of doing so might counter that perceived risk (Finucane et al., 2000). Within cybersecurity, positive emotions of convenience brought about by Internet-based services may reduce the perceived cyber-risks that one gets exposed to using the Internet (Finucane et al., 2000).

2.4.2 Protection motivation theory

Rodger initially developed the PMT in 1975 (Conner & Norman, 2005). In its inception, PMT was applied in the health care domain to study factors determining the person's intention and behaviour to protect themselves against the perceived threat or risk (Conner & Norman, 2005). The theory has since been applied in various domains, including tourism (Wang et al., 2019), extreme weather protection (Babcicky & Seebauer, 2019), and pro-environmental behaviour (Kothe et al., 2019). The need to study human behaviour in response to cybersecurity threats has compelled cybersecurity researchers to apply PMT within the cybersecurity domain (Li et al., 2019; Mou et al., 2022; van Bavel et al., 2019).

PMT posits that the judgement informs the protection behaviour that people practice of the perceived severity and likelihood of the threat (threat appraisal), such as their risk perception; and how equipped they perceive themselves to respond to the threat (coping appraisal) (Conner & Norman, 2005). PMT is a rational decision-making model and a

persuasive communication device that organisational leaders can use to influence them to perform protective actions/ behaviour to protect the organisations from cybercrime (Sommestad et al., 2015).

Sommestad et al. (2015) suggested that PMT could be used both where the desired actions or behaviours are voluntary or mandatory (Sommestad et al., 2015); there was an argument for the applicability of using PMT in cybersecurity because the original intent of PMT was for scenarios where people ought to make voluntary decisions to protect themselves rather than compliance requirement designed to protect the organisation (Chen & Zahedi, 2016). PMT could be considered an extension of the risk compensation model because in addition to threat appraisal and response cost considerations the model also considered additional factors that would motivate the person to take action against the risk, such as minimising residual risk exposure. These factors included how versed the person is in conducting such protective action, such as self-efficacy, and how they believe such action would effectively reduce the risk, such as response efficacy (Conner & Norman, 2005). The downside of the PMT model; however, was that it was more cognitively-based and does not explicitly consider the effect heuristics described above.

2.4.2.1 Fear appeals and threat appraisals

Fear appeals and their role in increasing people's threat appraisals have been considered in PMT-based studies within the cybersecurity domain (Burns et al., 2017; van Bavel, 2019). There are non-consistent observations on the effects of using fear to motivate users to adopt protective cyber behaviours. Some researchers contended that using fear appeal is an unsustainable approach to influencing cyber protective behaviour, and fear appeals lose their influence over time (Johnston et al., 2019). Empirical studies established that the adverse influence of fear appeal to cyber protective behaviour (Johnston & Warkentin, 2010; Posey et al., 2015). In the end, a study by Boss et al., in 2015 established that using fear appeals backfired because the resulting behaviour was the opposite of what was desired (Boss et al., 2015).

2.4.2.2 Coping appraisal

In 2016, an experimental study that involved functional magnetic resonance imaging

(fMRI) in measuring cognitive and affective reactions to fear appeals that emphasised the threat established that the user's self-efficacy to conduct recommended activities had a more positive influence on the induced intention and motivation to execute protective behaviour (Warkentin et al., 2016). While this initial finding was limited and could not be generalised because it was only played out in a laboratory setting, subsequent studies have imperially proven that coping appraisal has more influence than threat appraisal in influencing users' secure or protective behaviours (van Bavel et al., 2019; Li et al., 2019; Mou et al., 2022).

Coping appraisal has three core variables, such as 1) response efficacy, 2) self-efficacy and 3) perceived response cost (Conner & Norman, 2005). By deduction, perhaps if the user considers themselves capable of responding to the threat (response efficacy and self-efficacy) and considers the investment (for example, time) of carrying such response within their appetite, they will adopt a secure or protection action. Self-efficacy and response efficacy can be improved through interventions, such as cybersecurity awareness programmes (Li et al., 2019). To be effective, organisational cybersecurity awareness and training programmes should, therefore, have a reasonable balance between informing their employees about the cyber-risk and arming them with the know-how to handle such risks when they materialise.

2.5 Summary of literature review

It was evident from the literature that the risk of cybercrime (Bronk, 2015; Caldarulo et al., 2022; Sommestad et al., 2015) and insider-caused cyber incidents remain to be on the rise (Aloul, 2012; Crossler et al., 2013; Li et al., 2019; Pienta et al., 2020; Öğütçü et al., 2016; Song & Moon, 2020; Warkentin et al., 2012; Warkentin et al., 2016) and the influence is becoming even more systemic as dependencies on Internet-based services increase owing to increasing digital adoption (Burton et al., 2022; Caldarulo et al., 2022). While humans were often considered the weakest link in cybersecurity (Abraham & Chengalur-Smith, 2010; Aloul, 2012; Lee. 2021), it was also contended that they could play an important role in curbing these risks (Donalds & Osei-Bryson, 2020; Zimmermann & Renaud, 2019). As logical networks have been fortified through advancing technical security measures, humans could be trained to function as the last layer of defence against

cybercrime (Donalds & Osei-Bryson, 2020).

This critical function of humans in protecting the sociotechnical ecosystem has compelled several researchers in the last few decades to study human behaviour in cybersecurity (Cain et al., 2018; Crossler et al., 2013; Li et al., 2019; Donalds & Osei-Bryson, 2020). PMT as a risk-based behavioural model has been used in the cybersecurity space to study the motivations behind the adoption of protective cyber behaviours (Mou et al., 2022). A reasonable level of consensus has been obtained on that threat appraisal, and response appraisal in the PMT model was established to have various levels of influence on the resultant behaviour, with coping appraisal having a more pronounced influence on cyber protective behaviour (Li et al., 2019; Mou et al., 2022; Warkentin et al., 2016; van Bavel et al., 2019).

The use of fear to increase cyber-risk perceptions and to drive protective cyber behaviour yielded conflicting results in various contexts and studies (Johnston et al., 2019; Posey et al., 2015). The use of cybersecurity awareness has been used to drive policy compliance (Donalds & Osei-Bryon, 2020; Li et al., 2019; Liu et al., 2020; van Bavel et al., 2019) with further attempts to explore ways to make this awareness and training more effective (Johnston et al., 2019), little attention has been put to exploring the use of cybersecurity awareness and training to create awareness of the cyber-risk not only encountered by organisations but by employees too (Van Schaik et al., 2017).

Based on the literature reviewed in this chapter, a PMT-based model, depicted in Figure 1 below, was proposed. Cybersecurity awareness and training will shape cyber-risk perceptions from individual and organisational perspectives and impart knowledge on how to response to such risks. In return, both perceived risk and response abilities would influence the cyber behaviour that the user will adopt, with this also being driven by their perceived cost of conducting those cyber protective actions. Cost is not only limited to monetary value but time and effort.

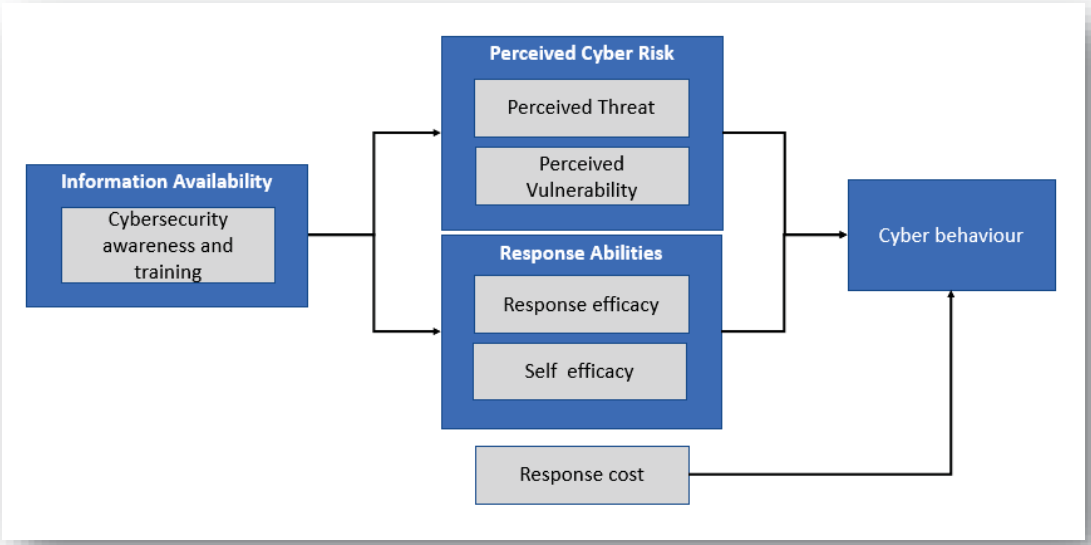


Figure 1: Protection motivation theory model

CHAPTER 3: PROPOSITIONS

After reviewing the literature on human behaviour in the cybersecurity space, the propositions are outlined in this chapter as perceived in the research.

3.1 Proposition 1

Cybersecurity awareness and training shapes employees on the organisational and individual cyber-risk perceptions

Cyber-risk perceptions are comparable to the threat appraisal of the PMT, where threat severity and vulnerability perceptions are formulated (Conner & Norman, 2005). Cybersecurity awareness is a form of information availability, an important element in the formation of amendment of a threat appraisal because without knowing of the threat, a person could not form a perception of the threat and their vulnerability to the threat (Gillam & Foster, 2020; Van Schaik et al., 2017). This proposition was made based on the understanding that when a person's knowledge and awareness of cybersecurity and cyber-risk is formed or improved within the work setting, not only would this would influence their perceptions of the cyber-risks encountering the organisation but their cyber-risk borne in the employee and personal capacities would also be shaped through the same awareness (Mou et al., 2022; Vishwanath et al., 2020).

3.2 Proposition 2

Individual cyber-risk perception functions as a lever for protective cyber behaviour in the workplace

PMT was first established in the personal health space, where there is a close personal association with the risk, and the adoption of this theory in organisational cybersecurity has been criticised based on personal proximity as the perceived risk is low (Vishwanath et al., 2020). Propositions 2 and 4 were made around this element of personal proximity to the perceived risk. The current proposition was based on the theoretical understanding of a personal association of individual cyber-risks. Employees are more inclined to take protective cyber behaviours to protect themselves against these risks (Johnston et al.,

2019; Menard et al., 2017; Mou et al., 2022).

3.3 Proposition 3

Organisational cyber-risk perception does not directly shape individual protective cyber behaviour

The relationship between intention and behaviour was smaller in the workplace, where behaviour is more compliance driven, which can be attributed to a low personal association between the perceived cyber-risk in the work setting (Mou et al., 2022). This is understood to be caused by the distance between the perceived risk and the person's actions (Vishwanath et al., 2020). The organisational identification theory has demonstrated a possible way this distance between organisational cyber-risk and employee cyber protective behaviour can be reduced by crafting the cybersecurity messages in a manner that joins people to the organisation, for example, using “our” instead of “you” (Johnston et al., 2019). Studies that focus on discussing this distance between perceived organisational cyber-risk and employee behaviour; however, remain nascent (Mou et al., 2022); therefore, this proposition is raised to assess this phenomenon in the South African financial services domain.

Where there is a distance between the person and the perceived risk concerning the relationship between the perceived consequences of such risk and its direct influence on the individual, the individual is less inclined to voluntarily adopt protective cyber actions or behaviour as illustrated through intrinsic motivation and using inclusive language.

CHAPTER 4: RESEARCH METHODOLOGY

4.1 Introduction

This chapter detailed the research design and methodology, including the population, unit of study, sample, data collection methods. The research instrument used for this study, together with the rationale for each design decision were outlined. Research legitimisation was also explained, and last, the limitations of this study and threats to reliability with quality controls employed are detailed.

4.2 Proposed research methodology and design

In this study, the researcher followed an interpretivism philosophy. In the interpretivism philosophy or paradigm, the research is centred on the data interpretation by the researcher, with the format of the data often in a non-numeric form (Kelliher, 2005). Scholars such as Saunders and Lewis (2018) advocate interpretivism as a more relevant philosophy for business and management research, especially when human-centric constructs, such as human attitudes and behaviour, are studied. This study examined the sociotechnical ecosystem in the business context, an intersection of social and technical aspects applied in the business domain (Pollini et al., 2021), making interpretivism a preferred lens to analyse a more nuanced insight into this study (Alharahsheh & Pius, 2020). Positivism philosophy use data from objective lenses with replicative and generalisation intentions. This was a less favourable philosophy for the present study (Saunders & Lewis, 2018).

The present study adopted the qualitative methodology, focusing on meanings shared by the research subjects and the relationships between those meanings to build insights (Goldkuhl, 2012). Qualitative research methodology is more aligned with the interpretive philosophy adopted for this study (Saunders & Lewis, 2018); therefore, the study followed qualitative research methodology through semi-structured interviews as the data collection method. Qualitative studies also allow for an in-depth study of a phenomenon, the employee perceptions around cyber-risk and the resultant behaviours, and why it was a suitable approach for the study.

The study followed inductive thinking to infer from existing literature and assess the

propositions made to prove them, expand them, or disprove them (Saunders & Lewis, 2018). Cybersecurity studies advanced in the last few years; however, literature still indicates that the phenomenon in this research, indicating context-based cyber-risk between work and personal settings, remains immature. Studies lack on this phenomenon before; therefore, inductive thinking would be an appropriate thinking approach (Mou et al., 2022).

Exploratory studies are embarked on to uncover new insights and observe the phenomenon in a new light (Saunders & Lewis, 2018). The cybersecurity behavioural research area is still in its infancy, and factors influencing employee cyber behaviours are not yet understood (Zimmermann & Renaud, 2019). It was, therefore, established that an exploratory study would be an appropriate approach to gain in-depth insights into people's cyber-risk perceptions and their resultant behaviours in the workplace and personal settings (Saunders & Lewis, 2018).

In cross-sectional studies, data from each subject are collected only once to assess the theoretical propositions outlined in Chapter 3. A cross-sectional design was selected not only because the researcher had a limited time to complete the research (Saunders & Lewis, 2018) but also because the study was not intended to measure or observe a phenomenon over time.

4.3 Population

The population of this study was people employed within the financial services industry in South Africa. Despite an adverse trend in cyber-breaches and cyber incidents in verticals such as manufacturing, health and education, the financial services sector still encounters high cyber-risk as it remains a lucrative market for cyber criminals (Kshetri, 2019) and the influence of cyber-breaches and cyber incidents in this domain have systemic adverse influence (Kshetri, 2019; Eisenbach et al., 2021). South Africa has observed a high increase in cyber-breaches over the past few years. A call for organisational leadership and researchers to focus on this area is required. Several listed financial services organisations in South Africa have itemised cyber-risk as a material risk. It is reported and governed by the respective boards of those companies (Standard Bank Group Annual Integrated Report, 2021; Old Mutual Integrated Report 2021, 2021; Firstrand Material Risk Factor Disclosure, 2022; Capitec Integrated Annual Report 2021, 2021).

4.4 Unit of analysis

For this study, the unit of analysis comprised the individual employees. The study was based on cyber-risk perceptions and behaviours from the perspective of people employed in financial services, and this was driven by the understanding that humans are the last layer of defence that needs to be tightened to counter the cyber-risks encountered by financial organisations in South Africa. (Salahdine & Kaabouch, 2019; Zimmermann & Renaud, 2019).

4.5 Sampling approach and description

4.5.1 Sampling method and qualifying criteria

Purposive or judgement, non-probability sampling was used to select the study participants. In purposive sampling, the researcher applied their own judgement based on defined criteria to select the sample from the population (Saunders & Lewis, 2018). The reason for using a non-probability sampling was according to the study objective, which was to gain nuanced insights than to empirically perform a statistical test, meaning probability and generalisation were not a requirement or according to the study objective. Purposive sampling, as a type of non-probability sampling method was chosen because it allows for flexibility while also guarding against selection bias as participants needed to meet the pre-defined criteria (Saunders & Lewis, 2018).

The study sample was selected from financial services employees from these departments: legal, risk and audit, marketing and sales, IT, finance and operations. These areas of the business were considered to provide reasonable coverage of the employee base, provided then types of roles they perform.

Participants were invited from the researcher's informal networks in financial services, and some participants were also requested to nominate other participants from their own networks. After ten interviews were completed, the researcher noted an underrepresentation of male participants—with only one male at that stage and attempted to recruit more males to participate. Two additional males were successfully recruited to participate in the study. While gender was not a defined criterion, it was important in this study to represent males and females.

4.5.2 Sample size

This study being qualitative, there was no intention to statistically assess any hypotheses to generalise the outcome of this study; therefore, a non-probability sampling method was appropriate. The researcher also did not have the time or resources to obtain an accurate population size (Sanders & Lewis, 2018).

Literature has revealed that a sample size of twelve participants is enough to reach data saturation in qualitative studies when working with a homogenous population, which was the case in this study (Guest et al., 2006). The sample size for this study was fifteen. All interviews were conducted before coding and analysis were initiated, owing to the researcher's time constraints. The homogeneity of the sample was on base. They were all professionals working in the financial services industry and were exposed to cybersecurity awareness and training. The participants, however, varied concerning their expertise in cybersecurity and adjacent domains, such as technology and risk. To mitigate the risk of the study not producing dependable results owing to insufficient sample size, the researcher increased the number of participants or the sample size to fifteen instead of twelve (Guest et al., 2006; Shenton, 2004).

4.6 Measuring instrument

In this qualitative study, the researcher was the main research instrument as the study was based on their interpretation and analysis of the data collected through semi-structured interviews to assess the theoretical inference-based propositions made in Chapter 3 (Maxwell, 2013). It is the nature of interpretivism paradigm studies to allow the researcher to derive meaning from the observations and perceptions of the collective participants of the study (Saunders & Lewis, 2018).

4.6.1 Interview guide

The interview guide included in Appendix 1 was designed following the long interview structure, where open-ended questions were designed with planned prompts to build on the main questions. (McCracken, 1988). The interview guide enables the researcher to collect the information from the participants, then used to assess the theoretical propositions in Chapter 3, with varying numbers of questions designed to allow for testing

of each of the three propositions. While the interview guide helped the interviewer run the interview in a structured manner and cover all the questions, the interviewer remained in control and, where required, could direct additionally questions to probe for more insights. They could change the sequence of the questions during the interview based on how the interview flows (Neuman, 2014; Saunders & Lewis, 2018).

Depending on the flow of the interview, the interviewer aimed to open the interview with biographical information to help to build rapport with the participant; however, the interviewer was also guided by the flow of the conversation with the interview as they kicked off the interview where certain cases, the interviewer went straight into the main interview questions before demographic questions. After the first interview, the first question in the main interview was amended to ask participants about their understanding of the term cybercrime to ensure a mutual understanding between the interviewee and the researcher about this critical concept of the research. Appendix 1 contains the full list of interview questions.

4.7 Data collection process

Interviews were conducted in English. The data were collected through semi-structured interviews held over a teleconference platform called Microsoft Teams. The reason for using teams was twofold—teams were a commonly used teleconference device in South African workplaces, meaning most participants had easy access to the platform and were also familiar with the technology (Bacchus, 2020). Online meetings experienced a strong increase in 2020, not only in South Africa, owing to the COVID-19 pandemic lockdowns (Mouratidis & Papagiannakis, 2021).

Online meetings are convenient and can provide a virtual presence with the potential to allow the interviewer to have some level of nonverbal cues during the interview; however, the full benefits of virtual presence meetings could not be obtained as some participants requested to have their videos turned off or they were compelled to, owing to network connectivity challenges. Limited nonverbal cues, such as the tone and pace of their voice, were observed (Saunders & Lewis, 2018). To compensate for the loss of engagement, the interviewer kept the camera on throughout the interview sessions to keep the interviewer engaged.

Most participants opted to run their interviews from the employer's corporate email addresses, with only four of the fifteen participants opting to conduct their interviews using their private email logical identity or email. Some participants opted to have the meeting during working hours, but there were a few scenarios where participants opted to have the interview either after working hours or over the weekend or public holiday. Before the interviews started, participants were reminded to be invited to the interviews in their capacities and not to represent their organisations.

The participants were reminded that their participation of voluntary, and should they want to withdraw from the interview or not answer any question they did not feel comfortable with, they could do so. Where participants had not provided the participation consent letter back to the interviewer, they were reminded to do so. All sessions were recorded using Team's native recoding capability, with auto-transcription enabled. After each interview, each recording and auto-generated transcriptions were moved to the researcher's personal Google Drive to ensure the confidentiality of the interviewees while meeting the university's retention requirements.

Before the interviews were conducted, a pilot-test interview was conducted. The main learning point from the pilot interview was that the researcher did not have probe enough and, therefore, the information obtained was limited, and the length of the interview only lasted for 20 minutes. Without changing the meaning, the interviewer made a note to amend the question in a manner limiting the chances of the interviewees not misunderstanding the question (Saunders & Lewis, 2018). This was a delegate balance that the interviewer needed to ensure that the interviewee understood the questions without leading them to a specific answer (McCracken, 1988).

4.8 Trustworthiness risks and mitigations

4.8.1 Credibility

One concern commonly raised by critics of interpretivism qualitative studies is their trustworthiness, with reasons such as researcher's biases on a selection of the subjects for the study and their interpretation of the collected data, provided the role played by the research in deriving meaning from the data (Cho & Trent, 2006; Saunders & Lewis, 2018). Credibility is a term used in qualitative studies comparable to the internal validity in

positivist, quantitative studies (Shenton 2004). Credibility considers several factors within the research setting itself that can threaten the validity of the results of the study (Saunders & Lewis, 2018). Other scholars use the term transactional validity to refer to the relationship between the researcher, the subject, and the data. In this paper, the term credibility is used (Cho & Trent, 2006). Credibility is one of the essential elements in ensuring the trustworthiness of the outcomes of the research and should not be taken for granted. The researcher applied these principles to improve the credibility of this study:

Subject selection: While a clear participation qualification criterion was defined upfront, the sample was also determined by the availability and willingness of the qualifying participants to participate in the interviews (Saunders & Lewis, 2018); however, when it became evident to the researcher after conducting ten interviews with only one male participant, male participants were explicitly recruited to participate in the study, which saw a slight increase by the time all fifteen interviews were completed, with three males in the total of fifteen participants. Other risks to the trustworthiness of the study or the research legitimisation were considered, and where feasible, mitigations were implemented.

Subject bias: cybersecurity is a sensitive topic for organisations, as such organisations do not readily or voluntarily share information about the condition of their cybersecurity. (Tonn et al., 2019). To encourage interviewees to share the information that will help to answer the research questions, they were assured of the confidentiality and anonymity of the shared information.

Accuracy of data provided by participants: To help participants share true data, the researchers applied several tactics. For example, at the beginning of each interview, it was reiterated that their participation remained voluntary and that they could at any point. They were under no obligation to answer all interview questions (Shenton, 2004). During the interview, where there was uncertainty about participant statements, the records were paraphrased based on their understanding. Participants were requested to confirm their understanding.

Apply learnings from the study: After learning from the first interview where the participants mentioned the definition of the term cybercrime, crucial terms in the study, such as cybercrime and cyber-risk, were first discussed with the participants to ensure a mutual understanding of what is meant by cybercrime and cyber-risk for the remainder of the

interview.

History: A recent event, such as a human-induced cyber breach within the organisation, the geographic location, or the industry vertical of the organisation the interviewee comes from, can alter their natural observations (Saunders & Lewis, 2018). The researcher kept themselves up-to-date on the cyber breaches leading to the interviews and be cognizant of this threat. A recent case should alter the interviewee's observations. During the interviews, two significant incidents may have influenced observations and attitudes to cybercrime. A bank in South Africa experienced an outage on their digital platforms that lasted over 24 hours. While the root cause was not made public, there were perceptions that a cyberattack caused the outage.

One of the main telecommunication companies in South Africa suffered a data leakage through their partner that saw their fibre customers' identification information, including physical addresses and copies of identity documents, exposed. The interviewer decided not to include participants from this bank. During the interview, the interviewer also requested an example of a South African major cyber breach or data leak that came to their mind, and none pointed to these recent incidents, which indicated that their observations and attitudes were unnecessarily affected by these recent events.

Interviewing skills: The researcher, who performed interviews in this study, is not an expert in conducting interviews. This indicated potential harm to the interview processes and the data collected through the interviews. The pilot-test interview granted the interviewer to practice opportunity to improve their interview skills (Saunders & Lewis, 2018).

4.8.2 Transferability

Comparable to generalisability or external validity in quantitative studies, transferability refers to the extent to which the outcome of this study can be replicated or applied in various settings (Shenton, 2004). The context of this study was employees in financial services organisations in South Africa, depending on a computer to perform their job functions within their respective organisations. While this study employed a non-probability sampling method (as it was originally intended) with a small sample size of fifteen participants, the outcome of this study can be transferable to theoretical propositions, therefore, establishing the existence of a phenomenon through those propositions

(Kelliher, 2005)

4.9 Ethical considerations

This research was conducted according to the University of Pretoria's Gordon Institute of Business Science (GIBS) ethical research codes. Copy of the ethical clearance email notification to the researcher in included in Appendix 2. The methodology chapter and the proforma interview guide were reviewed and approved by the GIBS ethical committee before the commencement of the data collection process. Participation in this study was voluntary, and participants were not renumerated for their participants. While anonymity could not be achieved as participants were interviewed and the interviewer had their name and contact information to arrange the interviews, participants were offered confidentiality. Participants were provided numerical pseudonyms, which have been used throughout this study to protect their confidentiality.

4.10 Research limitations

In addition to the credibility and transferability risks already outlined Section 4.9 above, these limitations are also identified:

- This study was conducted with participants within South Africa. Inference, generalisation, or applications of the results in various geographic regions may be impractical. It is expected that the data may contain geographical biases specific to South Africa. Further studies should be conducted in other geographic regions and compared to the study outcomes.
- The interviews were conducted over a teleconference medium, and video was not enabled in all the interviews either owing to participants' confidentiality concerns or poor network connectivity conditions during the interviews. This added more limitations to the researcher's ability to read nonverbal cues during the interview. There is a risk that participants may have had split attention and focus during the interview.
- From the methodology perspective, this research aimed to explore the relationship between constructs using a qualitative approach rather than a qualitative approach as the study aimed to obtain detailed insights to build on existing theories in this domain rather than to assess already established theories empirically. These relationships will require further empirical testing using statistical methods in future studies.

- The purposive sampling method is subject to researcher biases as the onus is on the researcher to interview participants from the qualifying population.
- The sample in this study includes participants with varying levels of exposure and proximity to the cybersecurity domain, which may cause non-consistency in the results. Future studies should aim to set the samples into more homogenous groups from the job type perspective.
- Attributable to the large population, this research focused on participants from legal, IT, finance, operations, marketing and sale and risk and audit to obtain representative views from cyber-risk perceptions and other related insights. While other studies established these among crucial business divisions to consider in organisations when studying employees, this may still be open to the risk of the study being representative.
- The cybersecurity domain is a sensitive topic, and participants may be uncomfortable freely sharing their observations. The interviews were conducted individually to mitigate this. Each participant was provided with an affirmation of confidentiality and that they were participating in their personal capacity and not representing their organisations.

CHAPTER 5: FINDINGS/RESULTS

Chapter 5 presents crucial findings from the data collected through fifteen (15) semi-structured interviews. The interviews were conducted between 8 August and 25 August 2022. Microsoft Teams platform was used and each interview was held during the time of day suitable for each participant. The average interview period was 44 minutes, with the shortest interview being 27 mins and the longest running 1 hour 14 mins. In the next sections of this chapter, steps taken to prepare the data are explained, and then the sample is described in detail before the results are presented, according to the three theoretical propositions of this study as presented in Chapter 3.

5.1 Data preparation

To prepare for the analysis of the collected data in text format required for a qualitative study, such as this one (Saunders & Lewis, 2018), Microsoft Teams auto-generated transcript files were uniquely renamed, and the contents of the files were edited to remove the identifying information such as names, fix spelling mistakes from the auto-transcription and add cosmetic changes, such as adding bold effects to interviewer's words in the artefacts. Each transcript file was named using the pseudo name, the type of the institution that they came from, a numeric identifier of the institution which starts at 1—incremental within each institution type. This is followed by divisions and the identifiers as presented in Table 1 below:

Table 1: Transcript naming

Pseudo name	Institution type	Institution no.	Division	Filename
Participant1	Bank	1	Legal	Participant1_Bank1_Legal
Participant2	Bank	1	Legal	Participant2_Bank1_Legal
Participant3	Bank	1	BDM	Participant3_Bank1_BDM
Participant4	Bank	4	RiskAudit	Participant4_Bank4_RiskAudit
Participant5	Wealth	1	IT	Participant5_Wealth1_IT
Participant6	Bank	2	Marketing	Participant6_Bank2_Marketing

Pseudo name	Institution type	Institution no.	Division	Filename
Participant7	Bank	3	IT	Participant7_Bank3_IT1
Participant8	Insurance	1	BDM	Participant8_Insurance1_BDM
Participant9	Bank	1	IT	Participant9_Bank1_IT
Participant10	Bank	3	IT	Participant10_Bank3_IT2
Participant11	Insurance	1	BDM	Participant11_Insurance1_BDM
Participant12	Insurance	2	OPS	Participant12_Insurance2_OPS
Participant13	Tax	1	FINOps	Participant13_Tax1_FINOps
Participant14	Insurance	3	RiskAudit	Participant14_Insurance3_RiskAudit
Participant15	Bank	4	COMM	Participant15_Bank4_COMM

A clerical error was observed when the transcriptions were loaded to Atlas.ti tool where Participants 2, 3, 4, and 5 did not follow the chronological order of those interviews. Table 2 below presents the correct order or the interviews. These transcripts were, however, coded according to the pseudo name numbering.

Table 2: Interview number and pseudo name mismatch

Pseudo name	Interview order
Participant2	4th interview
Participant3	5th interview
Participant4	2nd interview
Participant5	3rd interview

All transcripts were then loaded to Atlas.ti, and thematic and coding analysis was performed. First, initial coding was conducted to reduce the transcripts into digestible codes. One hundred and three (103) initial codes were defined. Codes were then revised and merged where they made sense to the researcher. After the second round of coding,

53 codes were present. The researcher then created categories using groups in Atlas.ti, according to the themes emerging from this study—cyber-risk perceptions, cyber behaviours, and cybersecurity. After this process was completed—62 codes, with each transcript having an average of 35 codes. The highest occurrences of codes per transcript were from participant 11, with 64 codes, whereas Participants 2 and 7 had the lowest code count of 34 each. The codes were then mapped to categories, indirectly mapping them to themes.

5.2 Sample description

The 15 participants of this study were employees from nine financial services organisations, with most participants coming from commercial banks (7), followed by insurance companies (4), and non-commercial banks (2), and finally, there was only one (1) participant from a tax company and one (1) from a wealth and investment company. Many large enterprises have a footprint across the country and, sometimes, beyond the borders of South Africa. Some participants work remotely, whereas some have a hybrid work setting; therefore, the geographic location was derived from their company headquarters. All participants came from organisations with their headquarters in South Africa, with 12 based in Gauteng and three in Western Cape province. With Gauteng as the country's economic hub, the numbers were not surprising.

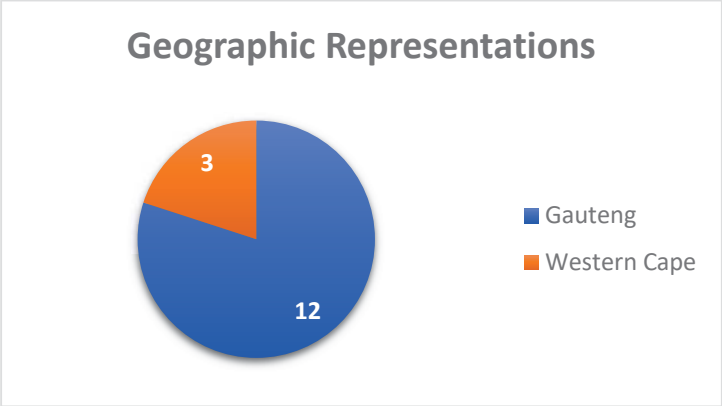


Figure 2: Geographic representation

Twelve of the participants have been with their employers for at least three years, with eight of those having at least six years of tenure. Given that some cybersecurity interventions, such as cybersecurity training, may be as less frequent as once per annum

in a certain organisation, the tenure of over two years would have afforded participants the to formulate or shape a perception of cyber-risk from the day-to-day work and the training and awareness communication received at their employment companies.

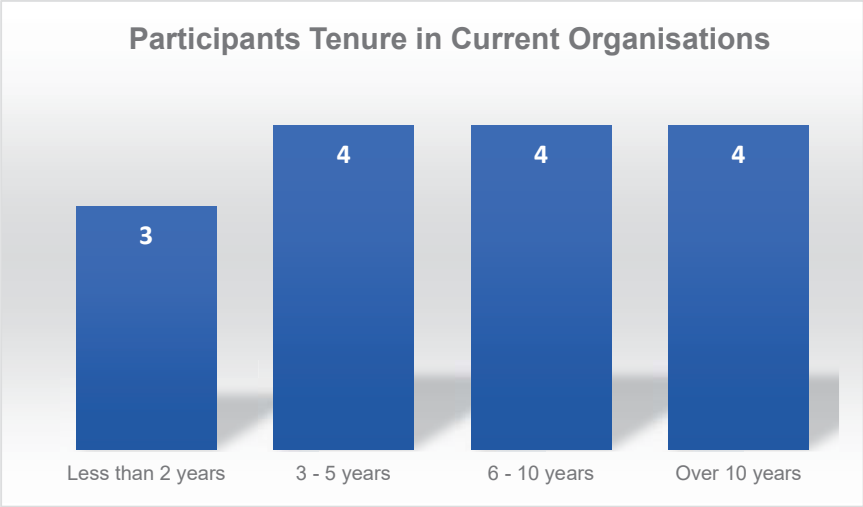


Figure 3: Participants' tenure

Of the three participants that have been with their employer for less than two years, two have been working in the South African financial services industry for more than five years, with the last one in this category emanating a small, non-financial (law) organisation. While the initial criteria for participation in this study required employment in the financial services organisation for at least two years, this participant was interviewed despite their not meeting that criterion as the researcher only learnt of their non-conformance during the interview; however, the insights from the interview with this participant compelled were perceived valuable.

The study aimed to obtain a collective observation from a reasonable representation of financial services in South Africa. The heterogenicity of the participants was not only considered from the organisations that they work at but also included divisions where they work, and it was expected that various divisions; therefore, job functions and responsibility levels would portray a collective view of employees' perspectives on cyber-risk and the resultant cyber behaviours. For this report, the count of participants from cybersecurity was included in the IT count, which may present an impression of an overrepresentation of IT participants, whereas only two of the four participants indicated as "IT" were from cybersecurity. The remainder came from business development (3), risk and audit (2),

legal, operations (2), marketing and communications (2), and finance (1).

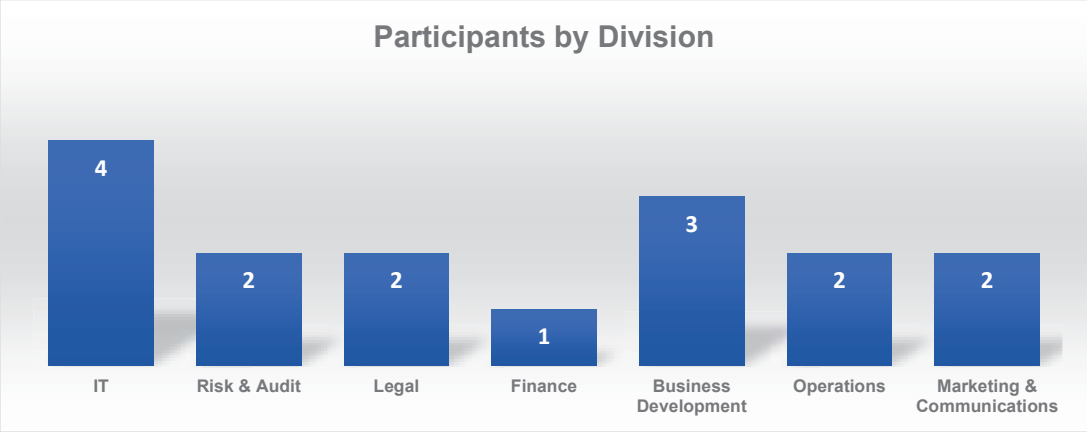


Figure 4: Participant division

From the seniority perspective, the participants spanned specialist level up to c-level. A specialist was defined by those employees with no direct reports, and they job titles included “analyst”, “practitioner”, and “specialist”, or were definite, such as “lawyer”. Middle managers were those participants with specialist-level employees reporting to them, and senior managers were heads of their functions or had managers reporting to them. C-level had the title with “Chief” prefix. Owing to a lack of availability of C-level participants, only one c-level executive participated in this study. The researcher was confident that a fair representation of senior managers (6) was sufficient to bring insights from the leadership perspective, while middle managers (3) and specialists (5) would provide insights from the ground.

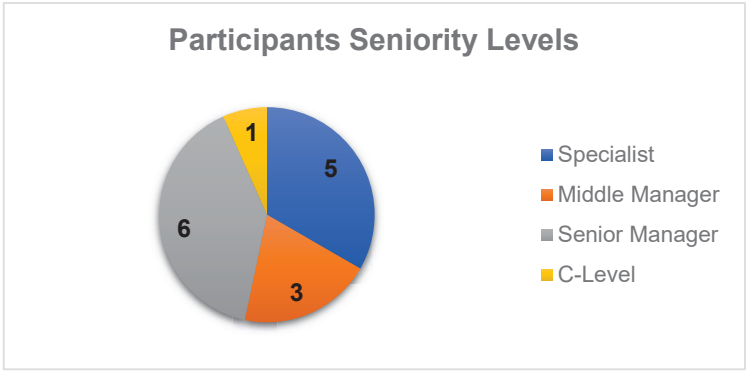


Figure 5: Participants’ seniority levels

Table 3 below presents the participants by organisation type, division and job titles:

Table 3: Participants' division

Pseudo name	Institution type	Job title
Participant1	Bank	Senior Legal Counsel
Participant2	Bank	Legal Counsel
Participant3	Bank	Business Development Manager
Participant4	Bank	Head of Risk
Participant5	Wealth	Business Analyst
Participant6	Bank	Digital Marketing Senior Manager
Participant7	Bank	Senior Project Manager: cybersecurity and IT Infrastructure
Participant8	Insurance	Head of Strategic Projects
Participant9	Bank	IT Asset Manager
Participant10	Bank	Project Manager: cybersecurity and IT Infrastructure
Participant11	Insurance	Regional head: personal finance
Participant12	Insurance	Actuary senior manager
Participant13	Tax	Chief operating office & chief financial officer
Participant14	Insurance	Audit manager
Participant15	Bank	Change practitioner

5.3 Findings and observations

A hybrid coding approach was used where the first round of coding was conducted almost independently of the model defined in Chapter 3. Categories and themes were then defined based on Chapter 3. In the second round of coding, similar codes were merged and where codes were renamed from the perspective of the model defined in Chapter 3.

The remainder of this chapter detailed findings against each proposition made in Chapter 3. The chapter was structured according to the emergent themes associated with each proposition summary indicated in Figure 7 below. Where a theme is associated with more than one proposition was discussed on its first occurrence. Where quotations were made throughout the chapter, the researcher used bold text to emphasise the quotations, and

this is their data interpretation.

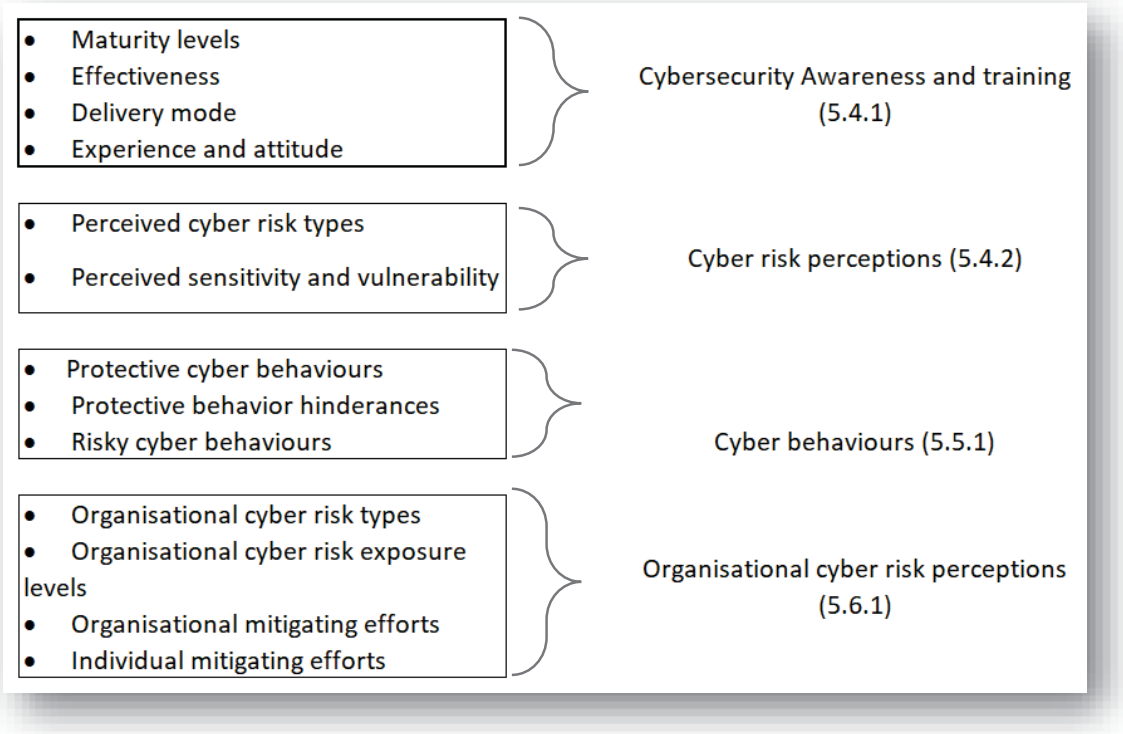


Figure 6: Emergent themes and proposition component alignment

5.4 Proposition 1: Cybersecurity awareness and training shapes employees on the organisational and individual cyber-risk perceptions

The first proposition related to the role played by cybersecurity awareness and training programmes that employees participate in their organisations and how this knowledge and awareness shapes their perception of the cyber-risk exposed to in their individual capacities as employees and in their personal capacity. Two constructs in this proposition, such as i) awareness and training and ii) perceived individual cyber-risk were explored according to the themes depicted in figure 6 above.

5.4.1 Cybersecurity training and awareness and training (CSAT)

Awareness and training form the input to the formation and enhancement of the cognitive

knowledge of the cyber-risk. Once the risk is understood, behaviour would no longer be independent of this knowledge. Participant 8 affirmed:

> "I think awareness is one of the best tools we have against cyber crime, right? Because if you don't know that you're vulnerable, then you there's no [way of] telling what could happen..".

5.4.1.1 Maturity levels

Most participants were employed with organisations holding high-maturity cybersecurity awareness and training programmes. Of the 15 participants, only four shared that their organisations did not have mandatory training as part of their awareness programmes. The bar graph below represents the code occurrences for low and cybersecurity awareness and training maturity levels. Lower maturity in cybersecurity awareness and training was coded from quotations, such as Participant 4 and Participant 13 who respectively alleged the subsequent about their organisation's cybersecurity programme:

> "So, there is training, but for me I think it's not robust enough, especially since the moving [to] working from home". ~ Participant 4

> "So, the thing is, it's done haphazardly. We've got a WhatsApp group and we will say listen, be mindful, be careful". ~ Participant 13

Figure 7: cybersecurity awareness and training maturity

5.4.1.2 Effectiveness

Perceptions of the effectiveness of the cybersecurity and awareness training to entrench

a cybersecurity-conscious mindset and behaviour were relatively high, as outlined in the bar graph below. Of the four participants that came from organisations with low maturity of cybersecurity awareness and training, only one reported that what they were exposed to was effective, and one other indicated that the minimal that they were exposed to concerning cybersecurity awareness and training was ineffective, whereas the other two did not comment on the effectiveness of the awareness and training they were exposed to.

> "I think it's quite effective. I think it's a regular communication with individuals within the organization to inform them about the risks of cybercrime and just to even educate them about what it is about? Why is it important? What are the repercussions if it were to take place? What does it mean for you as an individual and what does it mean for the organization and constantly updating us?" ~ Participant 12

> “I actually think it is achieving the objective because people are much more aware, you know, when we when I first started at this organization, I was so surprised that everybody was just clicking on my emails”. ~ Participant 14

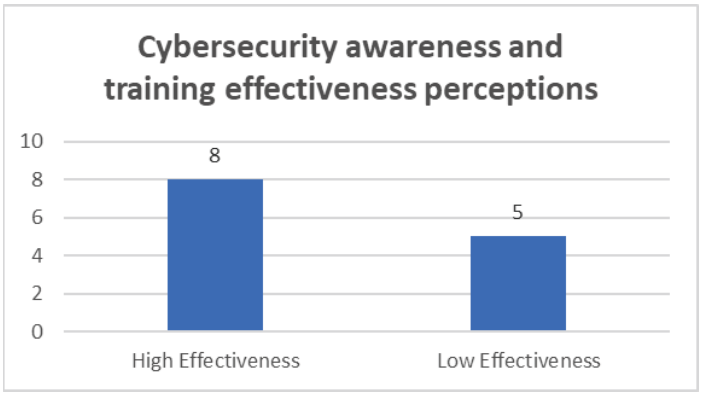


Figure 8: cybersecurity awareness and training effectiveness

5.4.1.3 Delivery modes

Concerning the delivery mode of the cybersecurity training, most participants indicated that in their organisations, it was delivered using online platforms in an asynchronous manner where they could complete the training in their own time, within the due dates. Only two participants reported that they had formal classroom training sessions on an annual basis. There was an indication that some participants believed that instructor-led

classroom options would be more effective when combined with the online option. For example, Participants 5 and 6 affirmed:

> "But sometimes you do it just so that we can complete it [online training]. But sometimes I think we do need face to face training" ~ Participant 5

> …and then you get a roadshow to a workshop or whatever. Very rarely do you get an impromptu master class or whatever; a place where you can go and actually learn and do it at your own pace and truly internalize it. I think that's what's missing. But they do try. Shame they send out even on my emails and I'm sure on Yammer we use Yammer internally. I'm sure there's a whole lot of information we must talk, knowledge that as a person" ~ Participant 6

Participants were often exposed to more than one mode of delivery. Figure 10 demonstrates the number of delivery modes coded from each transcript. The subsequent diagram depicts the occurrence frequency for each of the delivery mode codes

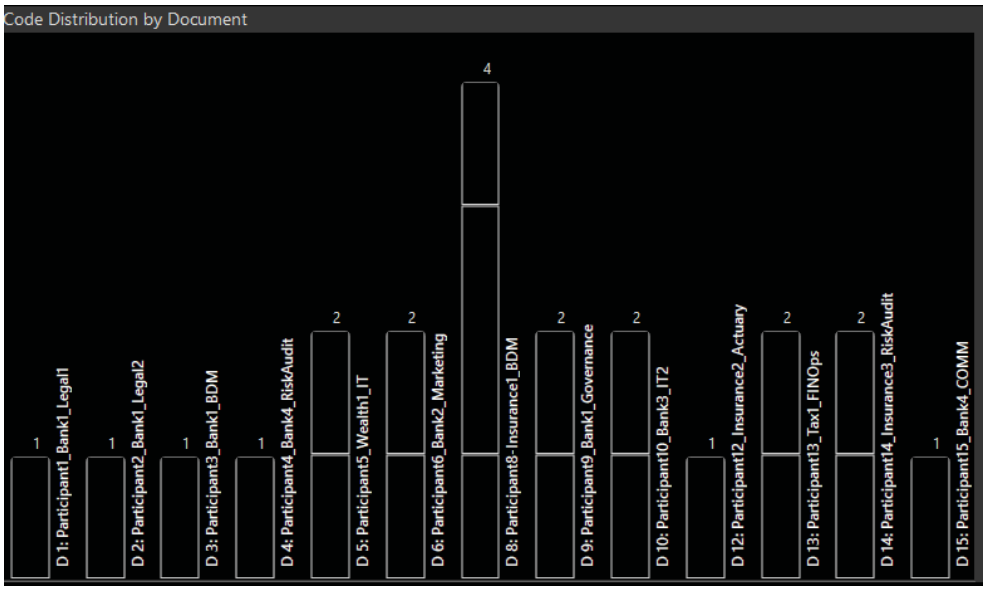


Figure 9: Code distribution by document

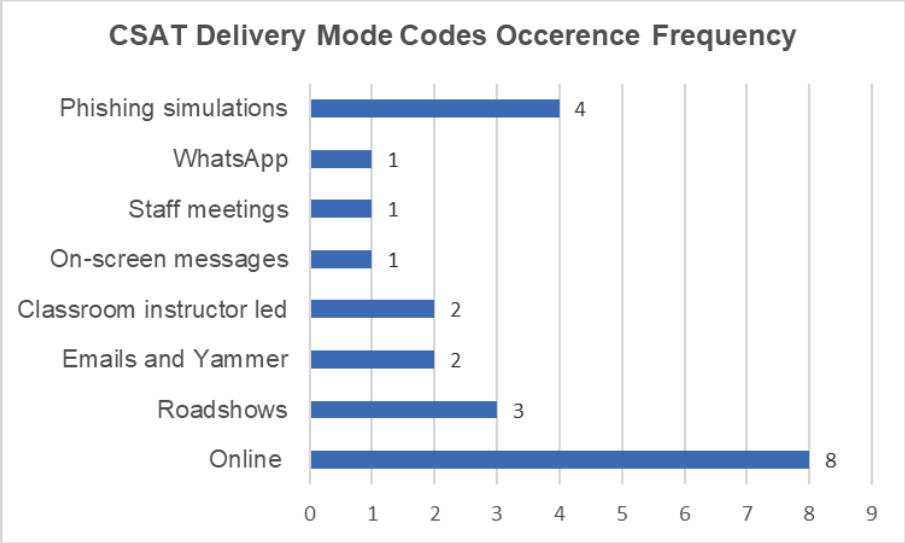


Figure 10: CSAT delivery mode code distribution

5.4.1.4 View and perceptions

Most observations of cybersecurity awareness and training programme perceptions indicate that employees have been exposed to from their respective employers were positive, with eight expressing positive observations of the programme at least once during the interview. There were; however, adverse observations which level up the positive observations expressed by eight participants, four of whom have also expressed positive observations and perceptions. Where an adverse observation was held with no neutralising view, the participant observed the programme as a tick box exercise, and they affirmed:

> "…we have mandatory cyber security training that talks about phishing and all these other things that I have forgotten about top of mind. But it's very much like these mandatory short trainings online that we do, and it's almost like a tick box exercise"
> ~ Participant 3

Positive observations were associated with perceptions of an effective cybersecurity programme as indicated in Figure 11 below.

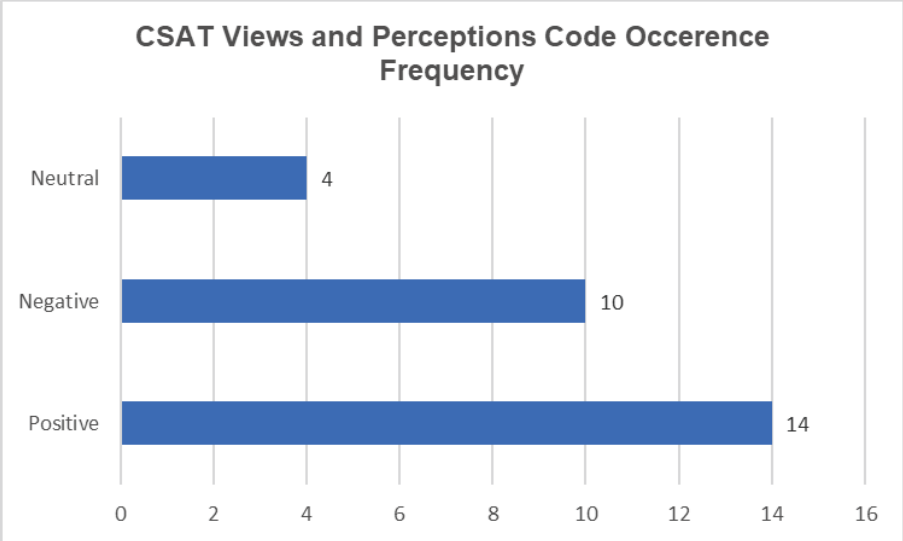


Figure 11: CSAT views and perceptions code occurrence frequency

Opposing observations were participants revealed positive and adverse observations and perceptions could be observed from a few participants, suggesting these participants did not hold strongly to each view. Responded 1 affirmed:

> "…So it's really difficult to concentrate online because you attend this audio training and then whilst you are doing something else on the side, so they are useful I think. But sometimes I think they're just playing lengthy and sometimes don't understand the concepts you know. Umm, but overall, they're useful, but it's just difficult because you're doing it online. You will be doing your other work as well". ~ Participant 1

Similarly, Participant 6 affirmed:

> "They're trying to make it teach you, but have fun and at the same time, because maybe you might remember faster… But you [must] remember that when I go on to compliance training, I'm wearing the hat that says I have to do this, or else I'm not [going to] get my bonus. So sometimes I worry if people truly internalize the education that is actually, supposedly being imparted". ~ Participant 6

Participant Pseudo Name	Cybersecurity awareness					
	Maturity	Effectiveness		Views and Perceptions		
Participant1	High		Low	Positive	Negative	
Participant2	High	High		Positive		
Participant3	High		Low		Negative	
Participant4	Low		Low		Negative	
Participant5	High			Positive	Negative	
Participant6	High		Low	Positive	Negative	Neutral
Participant7	High	High	Low	Positive		
Participant8	High	High		Positive		Neutral
Participant9	High	High			Negative	
Participant10	High	High		Positive	Negative	Neutral
Participant11	High	High			Negative	Neutral
Participant12	Moderate	High				
Participant13	Low					
Participant14	High	High		Positive		
Participant15	Moderate					

Figure 12: cybersecurity awareness and training analysis overview

5.4.2 Cyber-risk perception

A general observation shared by the participants was that all people with cyber presence were at risk, themselves included; however, some people had a higher sense of this risk, whereas others observed they would not make attractive targets to cyber criminals and are, therefore, had lower individual cyber-risk perceptions. For example, Participants 7 and 9 observed that they are less inclined to be victims of cybercrime:

> "…I shouldn't be hacked. So, I haven't had an I haven't been hacked even on my social media profiles". ~ Participant 7

> I'm not that interesting…. So why would anyone want to come for me? ~ Participant 9

5.4.2.1 Perceived cyber-risk types

Data loss and financial loss (including financial extorsion and digital fraud) are the two main perceived cyber-risks encountered by individuals and organisations. Identity theft

and social media identity hijacking—both subsets of data loss, were also among the frequently mentioned cyber-risks, having been in nine and 10 times among 13 of the 15 participants. System-level cyber-risks, such as system compromise and ransomware, were least mentioned, an observation that may be attributed to either lack of interest to the technical aspects of cyber-risks or a lack of awareness.

> "Other information that let's say they take my information and sell it to somebody or they clone my identit"~Participant13

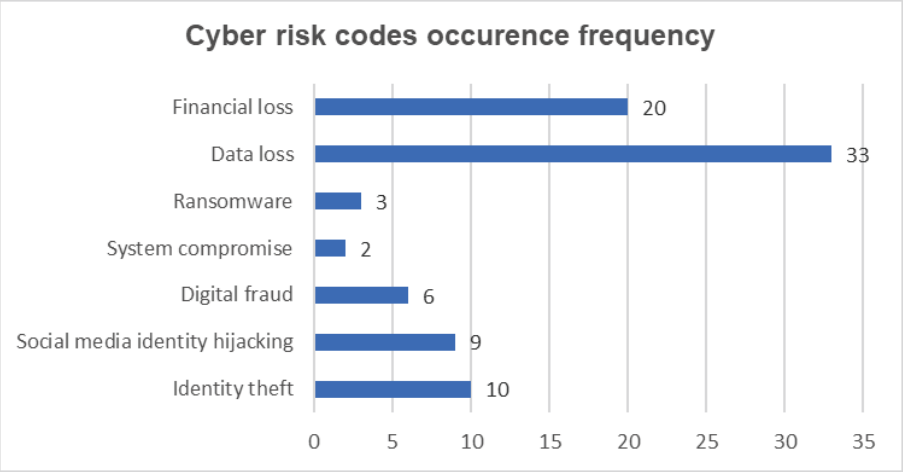


Figure 13: Cyber-risk codes occurrence frequency

5.4.2.2 Perceived severity and vulnerability

Participants perceived vulnerability to cyber risk was coded based on the researcher's interpretation of responses to questions about what they thought they would be an inclined to target for cyberattacks and whether they would be worried if they noticed their computer did not have anti-malware installed (Question 6 in Appendix 1). There was no clear cut between those with low individual cyber-risk perceptions and those with either high or moderate. Transcripts that held these opposing observations were analysed in depth to obtain the true sense of the participant's observations and perceptions of the individual risk. The interpretation applied here was that participants were that the highest risk perception is treated as the truth. For example, Participant 7 had shared low and high individual cyber-risk perceptions, with high individual risk.

> "So yeah, for me it's one of one of the things I'm sensitive about, making sure that I

keep my information very private" ~ Participant 7

"So, I've got more preventative measures… So yeah, because one of the things I do I when I get and a message that I'm not familiar with, I give myself time and read it and 90% of the time I just don't know. And I think if this is [going to] blow my phone, let it get blown, but it shouldn't. I shouldn't be hacked. So, I haven't had an I haven't been hacked even on my social media profiles". ~ Participant 7

Participant Pseudo Name	Individual Cyber Risk Perceptions (Vulnrability and Severity)		
	High	Low	Modertate
Participant1		Low	
Participant2		Low	
Participant3	High		
Participant4	High		
Participant5	High		
Participant6	High		
Participant7	High	Low	
Participant8	High		
Participant9	High	Low	
Participant10			Moderate
Participant11	High	Low	
Participant12	High	Low	
Participant13		Low	
Participant14	High		
Participant15			Moderate

Figure 14: Individual cyber-risks

The subsequent quotation from Participant 13 further illustrated that the low-risk perception could be linked to a lack of awareness of the risk. They affirmed:

"I basically do everything online banking is online and social media and yeah, basically everything. …I have to say that I've never, to be honest, I've never looked at cybercrime and social media as a potential threat".

When explicitly asked what the worst severity could be if they suffered cybercrime, the same participant (13) affirmed:

"So I think the worst would be financial influence. Umm, you know if they would defraud me with information, other information that let's say they take my information

> and sell it to somebody or they clone my identity. What I don't know won't do it. …Actually, I'm laughing because I'm getting nervous the more you ask the questions, the more, I think. I haven't thought about it. …I'm just thinking, Oh my goodness".

There was a common observation among the participants confirming an element of individual cyber-risk they inherit from their employment in the financial services industry. Access to personal data and the ability to make financial transactions with higher cyber-risk were crucial elements driving the inherited risk. For example, Participant 14 expressed a perceived higher individual cyber-risk they were exposed to owing to the role and the access they had because of their work role:

> "…our role, as you know, independent assurance providers, we have access to all of the systems because for me to provide assurance, I have to go in with my profile to see what's actually happening on the system… We have to make sure that, you know, we keep our credentials very close and very near because if somebody had to intercept us or our machine because we have access to all of the other systems and actual databases as well…"

Perception of an increased individual cyber-risk owing to personal or social association was only cited by Participant 8. This was included in the results because the researcher observed it as an interesting perspective but was not explored further as it was not core to this study. Participant 8 affirmed:

> "And I was telling a friend that I probably know of the most [of the] high earning people, or of that 1.5% in the highest earning people. So I think in the kind of roles and parts of the society that we find ourselves in now, there's always access to more of those people. So, I think you know we centrally have a high-profile people, high profile friends, high profile classmates, high profile bosses and leaders that we are connected to. So I think if I was to be targeted from that perspective, it would be to get access to that network of people that I also have and yeah"

There was a general shared observation that organisations have high cyber-risks except for participant 12, who indicated that the influence of cyber-risk on organisations is rather lower when compared to individual risk influence. The participant observation is that organisations can transfer most of these risks through cyber insurance covers, and as individuals, there is no leverage of this nature.

I think in terms of corporate, I think the consequences are big, but I don't think they're bigger than being targeted as an individual. I think well, I mean the worst that can happen, maybe they'll get into the company's data and maybe try and you know, elicit some funds out of that and maybe target the individuals and maybe there's some reputational risk. But you know, I think organizations have insurance against these things. Individuals don't. And I just think it's, I think the consequences are quite severe for the individual. They're likeliness, the likelihood of happening for individuals is probably low because you know it's widespread and targeting everyone. But I think the consequences are bigger"~ Participant 12

Participant Pseudo Name	Cybersecurity awareness						Organisational cyber risk perception
	Maturity	Effectiveness		Views and Perceptions			
Participant1	High		Low	Positive	Negative		High
Participant2	High	High		Positive			High
Participant3	High		Low		Negative		High
Participant4	Low		Low		Negative		High
Participant5	High			Positive	Negative		High
Participant6	High		Low	Positive	Negative	Neutral	High
Participant7	High	High	Low	Positive			High
Participant8	High	High		Positive		Neutral	High
Participant9	High	High			Negative		High
Participant10	High	High		Positive	Negative	Neutral	High
Participant11	High	High			Negative	Neutral	High
Participant12	Moderate	High					High
Participant13	Low						High
Participant14	High	High		Positive			High
Participant15	Moderate						High

Figure 15 - CSAT and organisational cyber-risk perceptions

5.4.3 Proposition 1 conclusion

To minimise subjectivity in the determination of aggregate or cyber-risk, the method depicted in Figure 16 below was followed. Most participants had high cyber-risk perceptions. In total, 11 had high cyber-risk perceptions, and only three had moderate perceptions of this risk. To a large extent, this aligns with the high maturity levels of the perceived effectiveness of cybersecurity awareness and training programmes that participants have been exposed to in their respective organisations, except for one case,

Participant 2, from an organisation with high maturity of cybersecurity awareness and

training programme, also perceived it to be effective but had moderate cyber-risk perceptions. Of the two people from organisations with low maturing cybersecurity awareness and training programmes, only had high cyber-risk perceptions. This individual's function as head of risk could be a contributor to this view. The participant from the organisation with moderate cybersecurity awareness and training, revealed high and low individual cyber-risk perceptions. This proposition is, therefore, confirmed.

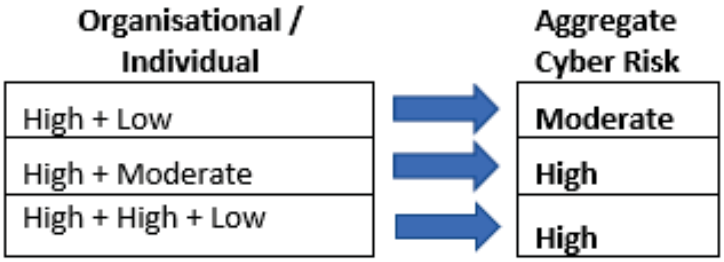


Figure 16: Aggregate cyber-risk interpretation

Participant Pseudo Name	Cybersecurity awareness						Aggregated cyber risk
	Maturity	Effectiveness		Views and Perceptions			
Participant1	High		Low	Positive	Negative		Moderate
Participant2	High	High		Positive			Moderate
Participant3	High		Low		Negative		High
Participant4	Low		Low		Negative		High
Participant5	High			Positive	Negative		High
Participant6	High		Low	Positive	Negative	Neutral	High
Participant7	High	High	Low	Positive			High
Participant8	High	High		Positive		Neutral	High
Participant9	High	High			Negative		High
Participant10	High	High		Positive	Negative	Neutral	High
Participant11	High	High			Negative	Neutral	High
Participant12	Moderate	High					High
Participant13	Low						Moderate
Participant14	High	High		Positive			High
Participant15	Moderate						High

Figure 17: CSAT and aggregated cyber-risk perceptions

5.5 Proposition 2: Individual cyber-risk perception functions as a lever for protective cyber behaviour in the workplace

5.5.1 Cyber behaviours

5.5.1.1 Protective cyber behaviours

All participants in this study have indicated that they practice protective cyber behaviours, as observed in Figure 18 below. A varying sense of intentionality in applying cyber protective behaviour was observed from the participants. On one end of the radar, some believed they could “only do so much” as end-users and service providers needed to ensure that they were protected, and there were those who were highly intentional about being precautious in their cyber behaviours. For example, Participant 1 displayed less intentionality in their cyber protective behaviours, and this was expressed:

> “There's so much we can do. If your password is down tight, you rely on bank OTP's, So I mean, there's only so much you can do…” Participant 14 emphasised their intentional cyber protective behaviours and affirmed:
>
> And so personally for myself, when it comes to my identity specifically, I'm very cautious in terms of when I release my ID number for instance if I go up to visit my friend and you know, they ask for my ID number at the gate, I refuse to give it or give a fake number because I don't know where that is [going to] land. And second is if I have a copy of my ID and you know, it's needed for a certain application. I first want to understand where this information [going to] be going to and who's [going to] be housing it. So that you know my records are safe. And then I suppose when it comes to my personal information, all of it. I actually have passwords on all of my PDF documents, so even in the event that you have to get it forwarded to someone, you're [going to] have to have a password for it, which I never shared together with the with the file. I suppose lastly, so I have two factor authentication on all of my main like social media accounts including my banking profile… So personally, I'm very weary and I'm extra cautious about it because I know that you know there's a lot of opportunities for cybercrime and for the way that people can penetrate and use information. So, because I'm hyper aware and conscious about it, I tried to put these safeguards in place as much as possible..”. ~ Participant 14

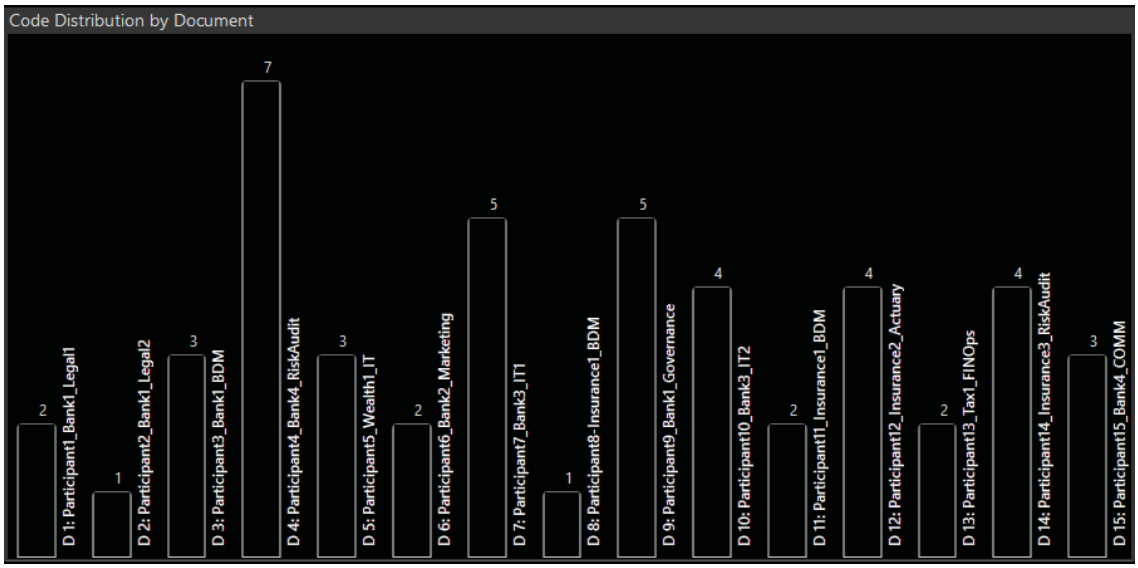


Figure 18: Protective cyber behaviour code distribution per transcripts

Some participants indicated an elevated level of protective behaviour by applying actions less involved, such as checking email validity than password protecting their documents or ensuring that they have multifactor authentication enabled than actively applying password protection on the documents they perceive sensitive. For example, participant 11 affirmed:

> "…like I said, I'm probably not the most vigilant person. Uh, in essence, I just do the bare minimum".

The same participant believes that they have a perception of high cyber-risk about themselves but confesses to not being the most careful person or intentional about practising protective cyber behaviours. He is a senior manager in their organisation, heading a department of 400 employees with access to sensitive personal information for their clients. Their observation was that being attacked for cybercrime is more a question of "chance". They affirmed:

> "I probably am [an attractive target for cybercrime]. I think I was saying that I'm not the most careful. I'm not necessarily the type of person that is over cautious. I mean, I will give my bank card to my friend to go swipe when we are having lunch or at a bar or whatever. I don't mind giving even a work laptop to someone else to do whatever they need to do for it. So, I'm not definitely not the most vigilant person. But I think I probably make a very attractive target to be honest…. So, I think these

> guys[cybercriminals], maybe they use a a sort of spray and pray approach. They just do these things to a lot of people and then once someone bites, then that's that". Elaboration added.

When expressing their behaviour around protection against phishing attacks, which involves actions not highly involved, such as checking the source of an email, they expressed extraordinarily strong observations of how they protect themselves; they affirmed:

> "I'm very strict at looking out for the e-mail address of the source and actually thinking twice as to in the normal course of business, would I be getting someone sending me an e-mail to ask for the information that is being asked".

5.5.1.2 Risky cyber behaviours and hindrances

While all participants have reported practising protective cyber behaviours, there were a self-reported practice of risky cyber behaviours such as password reuse or contravening their organisation's cyber and information policies, such as not password protecting files with sensitive information. The decision to adopt a certain action or behaviour is taken case-by-case, and where the employee perceives their effort in to conduct a protective behaviour outweighs the anticipated protective value, they would adopt a behaviour that may be risky. The subsequent quotation illustrates this cost-benefit analysis:

> "I don't know. I have no clue. I just get mad and I've even found a workaround for that because now I'll print as PDF because I can't wait. I can't do the whole run around. I'll open the document. I obviously have the password, I'll open it, print as PDF, send the customer the PDF version that is unprotected which sort of defeats the actual purpose" ~ Participant 3

> "But it I think we have a very short tolerance and patience some of us because it hampers my productivity". ~ Participant 6

The graph below demonstrates co-occurrences of known generic hindrances, lack of change management of cybersecurity controls, and perceptions of security controls as obstructive and risky cyber behaviours. Were there the self-reported practice of risky cyber behaviours, there is the presence of generic hindrances. Perceptions of lacking change management or communication on cybersecurity controls and obstructive security do not always cause risky behaviours.

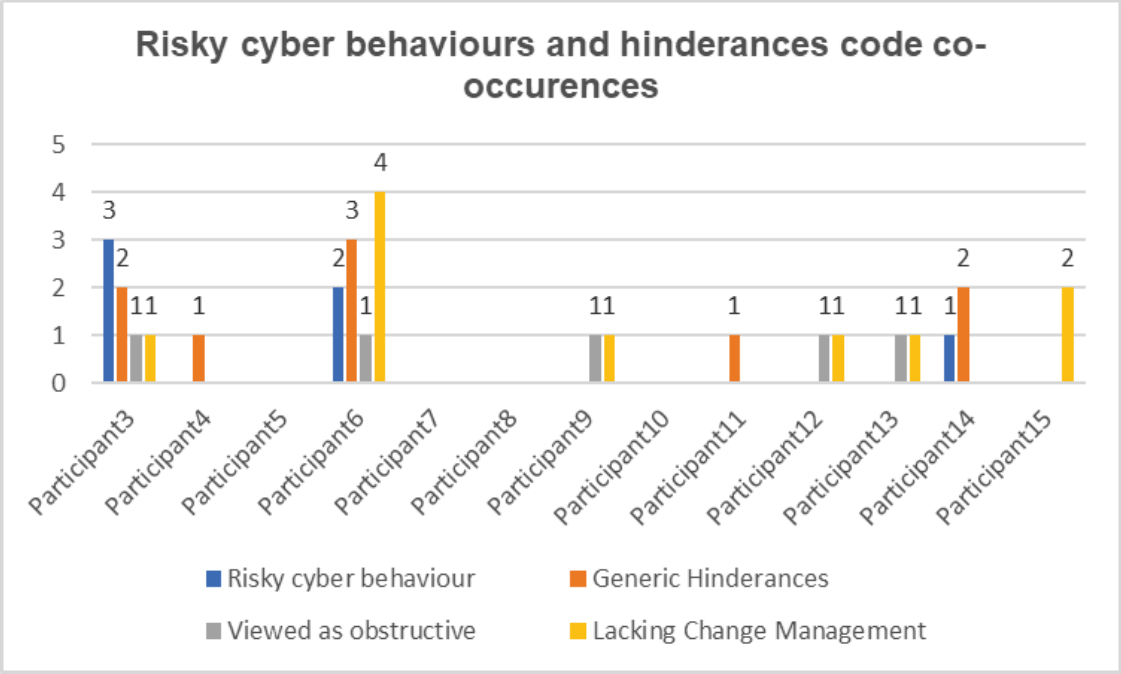


Figure 19: Risky behaviours related to codes

5.5.2 Proposition 2 conclusion

Risky cyber behaviours were not mutually exclusive with protective cyber behaviours. The decision to adopt an action or behaviour was conducted on a case-by-case base with elements such as perception of the required protective actions concerning its effectiveness in achieving the required protection and its influence on the employee's achieving their core mandate. Cyber behaviour is an ongoing cost-benefit analysis, where such observations and perceptions of cost (effort) and benefit (protection) can be improved through communication and training. Figure 19 in Section 5.5.1. above indicates that risky protective behaviours were only prevalent where employees were perceived to have generic hindrances, security was perceived as obstructive to productivity, or the security measure was not communicated.

There also seem to be an element of personality that played a role to the extent of cyber behaviours; for example, cyber-risk sensitive or paranoid people, such as Participant 7, 8, 9 and 14 were established to have higher reports of protective cyber behaviours as indicated in Figure 20 below. Where they practised risky cyber behaviours as directed in Section 5.5.1.2 above, they applied to compensate measures. For example, they

mentioned applying a grain of salt to the password that they reuse to have some level of uniqueness and they also relied on self-service password reset when they forget the password.

> "I always do like once a week. And restart my computer. I do a full scan, so I go into the security app and I said, you know, do a full scan of the computer to see if these antiviruses or attacks. No, I'm very. I'm super paranoid". ~ Participant 14

> "But sometimes it's a bit daunting … I just try to make it a memorable word and associate it with that kind of website in some shape or form, just so that it can jog my memory as to what the password is. So, I've been trying to keep it in my head, but with all fairness I request reset password more often than any other". ~ Participant 14

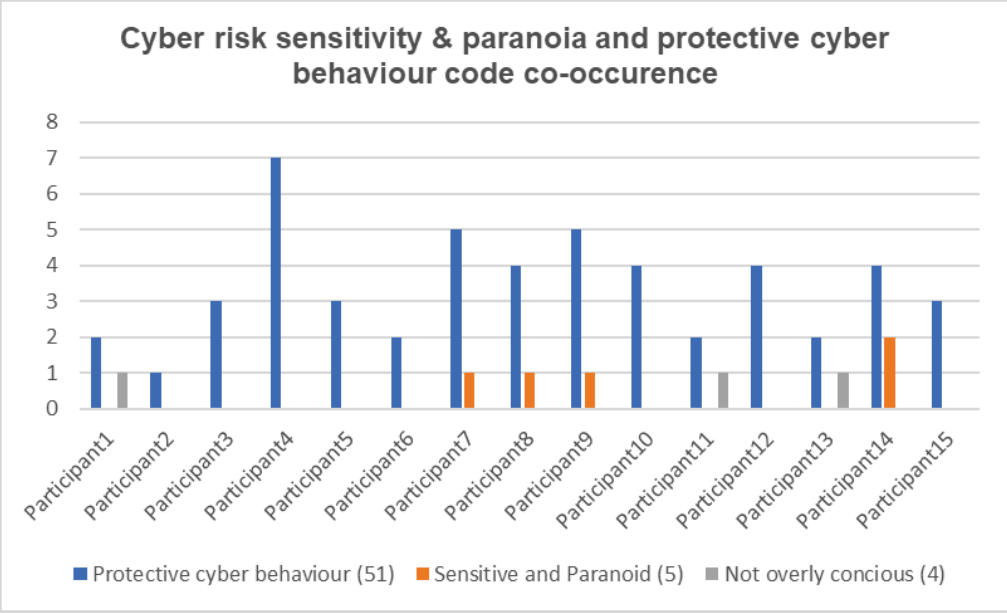


Figure 20: Sensitivity and paranoia and protective cyber behaviour code co-occurrences

The high individual risk perceptions seem to shape protective cyber behaviours. The three participants interpreted to have low individual cyber-risk, such as participants 1, 2, and 13, all shared fewer ways they ensure cybersecurity in their lives. Interestingly, these participants did not share practising risky cyber behaviours, suggesting a possible lack of awareness of actions that may increase their cyber-risk exposure. Having high individual cyber-risk does not; however, seem to suggest that employees will avoid risky cyber

behaviours. Risky cyber behaviours, as directed in Section 5.5.1.2 above, seemed taken on a transaction basis, based on the cost-benefit analysis for that scenario rather than an approach to cyber behaviours. This data suggests an amendment to the proposition made in Chapter 3, amended as follows:

Original proposition: Individual cyber-risk perception will act as a lever on protective cyber behaviour in the work environment

Amended proposition: Individual cyber-risk perception will act as a lever on protective cyber behaviour in the work environment, provided the employee understands the value of such behaviour and anticipated benefits of adopting the protective behaviour outweighs the required effort.

Important Note: In Figure 22, Individual cyber-risks are represented in numeric values with a high as 3, moderate as 2 and low as 1.

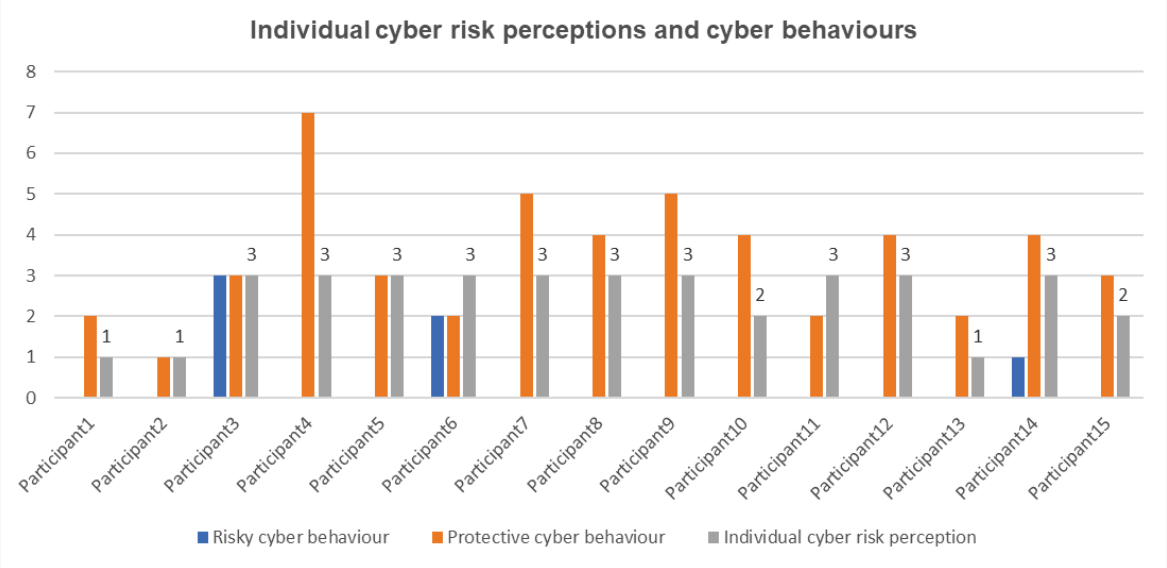


Figure 21: Individual cyber-risk perceptions and cyber behaviour

5.6 Proposition 3: Organisational cyber-risk perception does not directly shape individual protective cyber behaviour

5.6.1 Organisational cyber-risk perception

5.6.1.1 Organisational cyber-risk types

Data loss and financial loss, and the resultant reputational damage were directed at some high-influence cyber-risks encountering organisations. All these organisational cyber-risks seem interrelated. For example, lost data could be sold on the dark web for financial gain. The data would subsequently further attack the users or defraud them (financial loss). The financial loss was mostly attributed to a loss in customers resulting from fraudulent activities against customers or organisations themselves or soliciting a ransom for withheld data, all of which would have caused reputational damage to the organisations. Examples of quotations that illustrated these observations from the participants are:

> "Working for a bank. I mean, if someone hacks the Bank and gets hold of client information that would be very detrimental for the bank and the people that information belongs to. Not only will the bank lose clients because of that, people might also lose their hard-earned money, … So, in that sense for an organization, cybercrime will affect them and their reputation and also their revenue. So, it's very important for them to protect themselves from cybercrimes because it will be very detrimental". ~ Participant 9: IT Governance Specialist

> "…at the end of the day if I have exposed the bank and there's reputational… risk involved…" ~ Participant 7, cybersecurity Project Manager

5.6.1.2 Org cyber-risk exposure levels

The perceived high organisational cyber-risk was primarily illustrated by relatively strong observations against the concept of bringing your own device (BYOD), with participants arguing this practice unnecessarily exposes organisations to higher levels of cyber-risk as individual devices would not have high levels of protection. These strong observations BYOD based on risk were held by 12 of the 15 participants.

> "I'm totally against it. I think you know a work laptop should be for work and your personal laptop should be enough for you for your personal stuff. And the reason for this is that with the company laptop, you can be excessive, got that assurance

> to say, you know there's [malware protection] installed and it's up to date…" ~ Participant 10

> "It's a big no, so I think. Is the reason why companies give you their own hardware to access their systems? And I think the sort of defence mechanisms that are inherent in those sorts of devices will not be on your personal sort of laptop, so things like encryption and the antiviruses of the strength of an organization. Yeah, well, that would unlikely be on your personal laptop. So I would not recommend that". ~ Participant 11.

The remaining three participants are open to the concept provided it comes with mitigating controls, and the observations reflect that BYOD can enhance productivity.

> "I think they should be allowing it to the extent that it's appropriate. Security systems in place on the device itself… I think there should be allowing it because it just opens up the flexibility to be able to. Do your work wherever and whenever you want to". ~ Participant 12

5.6.1.3 Organisational mitigating efforts

With perceptions on the sufficiency of the mitigating controls that financial organisations in South Africa and, by implication, the residual organisational risk remains in these organisations, there was a split in observations. These ranged from those that believed that organisations were doing enough to mitigate the risk, those that believed that organisations were not doing enough to protect themselves and their customers from data loss. Some observed that while organisations are undertaking a lot, it would never be enough.

One participant, a senior manager of actuary services at an insurance organisation:

> (Participant 12) affirmed: "…I think the work is being done, but I don't think it's enough".

Some participants, such as Participant 15, had stronger adverse observations about the cyber-risk mitigation efforts that financial services implemented, and their observations seemed to stem from the recent data breaches that South African financial services organisations have suffered recently. Participant 15, for example, affirmed:

> "…So what surprises me is that those are big institutions that I mentioned… These

> are huge institutions with like 30, 000 people or 300, 000 people working for them, and God knows how much of the country's money they are holding in assets. I can't understand why they haven't done better. That's what gets me. …But it's just that these are large organisations. And you would think that they have a big focus on this... These are not start-ups" ~ Participant 15: Change Management Practitioner

A moderate observation reflects that participants contended that organisations are doing enough to protect themselves against cybercrime; however, ever-increasing complexities would always undermine those efforts, and the risk would, therefore, prevail. For example, Participant 13 emphasised the internal complexities, and they affirmed:

> "For the banks and I know the security is insane on their computers. But… with all those thousands of people working for the banks, I don't think they'll ever be able to fully control it".

Participant 8—a programme manager in business development manager of an Insurance firm, affirmed:

> "I think the more data that exists in the world, the more complex the issue becomes because criminals can come at it from any angle …"

Participants raised questions about whether organisations are keeping up-to-date with those ever-increasing complexities. For example, Participant 3 commented about a common technical security control of blocking USB ports for data storage on computers as dated and not according to the current form of the risk where data can be stolen through a plethora of mechanisms other than using the USB ports. They affirmed:

> "…It [blocking USB ports] was a wall that time. It was the only way to get like data and maybe on a larger context the USB thing and maybe having putting hard drive, maybe if it's stealing that [is] serious loads of data; yes, it is still good practice, but it's literally it was a wall back in the day, it's a hurdle now…"

5.6.1.4 Individual mitigating efforts

Concerning technical protective measures applied on the work-issued devices, a sense of personal distancing from the responsibility of ensuring their effectiveness regardless of their self-efficacy to do so. For example, Participant 1 appeared to have low self-efficacy in carrying protective actions technically oriented alleged the subsequent when asked if

they would be concerned if they noticed that the work laptop had no malware protection, they laughed and affirmed:

> “In the past four years I've been here, I've never thought about that. For me, it's never been a concern, even a thought so for me, it's not my role. So, if IT gives me the laptop, they are in charge of installing whatever they need to install. So, I don't even know how antiviruses work. So, I'm assuming that everything will be done on their side.... So, I'm assuming when the system updates or reboots or when I connect in the office network, I don't know, maybe that still cleans itself, but for me, I've never seen. It's not bothering me.”.

Despite their higher self-efficacy in technically oriented protective actions because they shared that they would apply technical protective measures on their personal device. They were clear that they would not be bothered to do anything about confirming the effectiveness of malware protection on their work device. For example, Participant 9 affirmed:

> “I'd hope they know what they are doing because I don't do any personal things on the work laptop, so if anything gets stolen or if hackers access things they are not supposed to, they would have to blame themselves. I hope that they know what they're doing if they disable antivirus, I'll just leave it to them. They're the experts”.
> ~ Participant 9

5.6.2 Proposition 3 conclusion

All participants in this study observed that financial organisations have high exposure to cyber-risks. The nature of these risks was largely attributed to customer data confidentiality compromise than to the operational influence perspective. Some employees perceived people that would be targeted to compromise the organisations to be people with attributes they did not share. This included untrained personnel, older people, children or people non-tech savvy. This observation subtly excluded the participants from the “high risk” list, which could suggest some patterns noticeable from the bar graph in Figure 22 below; where for example, Participants 1, 2, 11, and 13 had high organisational cyber-risk perceptions and self-reported lower protective cyber behaviours. The count of protective cyber behaviours is only one indication, but the bigger part of this indication is the broader interpretation of the transcript. There were exceptions regarding distancing from the organisational risk, for example participant 11 shared that

he would make an attractive target to cyberattacks by the type and amounts of data they had access to through their organisations.

> "People might think I have access to that particular financial services company's funds in some other fashion. And I probably want to rank plays into that as well. So, they might think … scamming me, they will have access to my financial institutions data. Which is invaluable. Which is probably the most expensive and the most important thing". ~ Participant 11

Important Note: In Figure 22, organisational cyber-risks are represented in numeric values with high as 3, as moderate as 2, and low as 1.

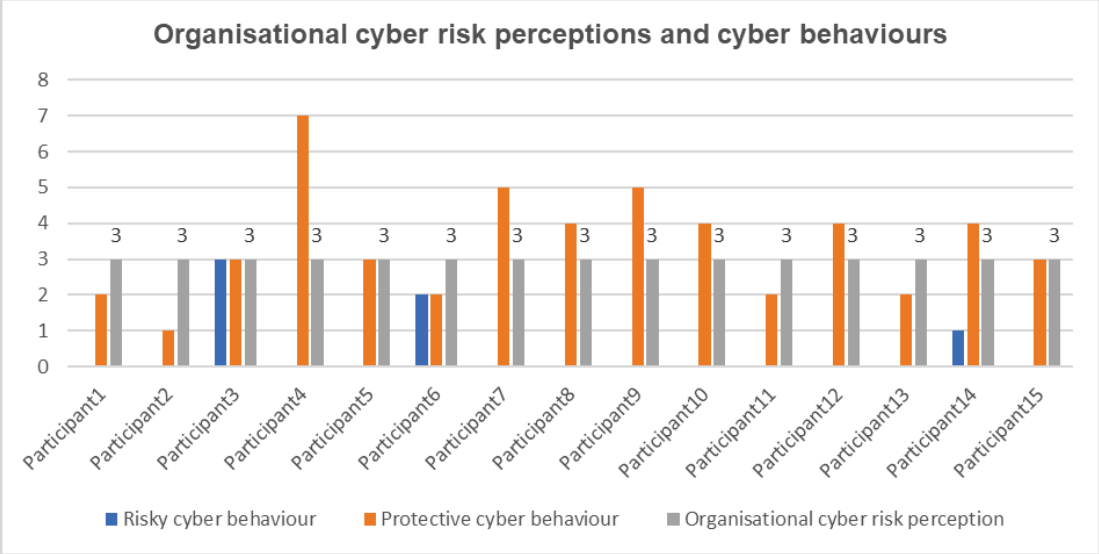


Figure 22: Organisational cyber-risk and cyber behaviours

There does not seem to be a relationship between organisational cyber-risk perceptions to employee cyber behaviours. This lack confirms the theoretical proposition made in Chapter 3.

5.6.3 Data analysis conclusion

In this section, the collected data was analysed to seek a response to the propositions made in Chapter 3. Propositions 1 and 3 were confirmed, and Proposition 2 was amended. In the next chapter, these results will be synthesised against the theory from the literature review conducted in Chapter 2.

CHAPTER 6: DISCUSSION OF RESULTS

This chapter continued to link the data obtained from the semi-structured interviews analysed in chapter five with the literature reviewed and presented in chapter two. Each proposition was reviewed against the literature with the aim of either confirming, amending or rejecting the propositions made in chapter three based on the reviewed literature. In the conclusion of the chapter, a revised model is presented, reflecting additional insights.

6.1 Discussion of Proposition 1: cybersecurity awareness and training will shape employees on the cyber-risk perception

Proposition 1 was made based on the premise that cybersecurity subject knowledge and awareness play a role in shaping employees' individual cyber-risk perception. The main construct in this proposition were: 1) cybersecurity awareness and training and 2) cyber-risk perception.

6.1.1 Cyber-risk perceptions

Literature emphasises that individuals encounter cyber-risks in their personal capacity and their capacity as employees (Cain et al., 2018). Cyber-risks were found to defined in literature as those information and technology risks suffered by individuals, organisations, and national states regarding a compromise of the confidentiality, availability, and integrity (Aldasoro et al., 2022; Strupczewski, 2021). This risk could severely affect organisations and individuals, including financial loss, and reputational damage (Aldasoro et al., 2022). To individuals, the influence could also include health and social influence too (Lievens, 2014; Pienta et al., 2020; Shahria et al., 2020). Older generations and those non-tech savvy or untrained in cybersecurity have higher levels of cyber-risk Caldarulo et al., 2022).

Identity theft was indicated as a type of cybercrime that could cause financial loss or reputational damage, such as where the identity is used to commit activities socially or politically unacceptable, such as soliciting money from unsuspecting victims that would otherwise trust the person whose identity was stolen (Irshad & Soomro, 2018; Shahria et al., 2020). From the individual financial loss perspective, cybercriminals could perform adverse activities, such as credit facilities using the victim's identity, and, therefore, subjecting them to pay a credit they would have never used (Lai et al., 2012; van de Weijer

et al., 2018). On the organisations's side, financial loss influence can result from operational disruptions, time and effort to respond to the cyber incident, digital fraud, regulatory fines and customer loss owing to lost brand trust (Aldasoro et al., 2022). Social-oriented cyber-risks observed from the literature include privacy violations, reputational damage from identity theft or exposure of sensitive information, embarrassment, cyberbullying, cyberstalking, and online harassment (Caldarulo et al., 2022; Shahria et al., 2020).

Key types of perceived individual cyber-risks from the findings included identity theft, privacy compromise, financial loss and reputational damage, while from the organisational view, loss of customer data was the most prevalent perceived cyber-risk. Concerning the extent of perceived individual cyber-risks, there was a strong observation that everyone with a cyber presence is at risk against cybercrime, with only a few indicating that they have higher cyber-risk perceptions than other people. There was; however, a common observation that the elderly and those new to jobs who have no exposure to cybersecurity training and hype, their social media presence and activities were more at risk.

This perception suggests that participants perceived themselves to have a lower or moderate residual risk because they did not fall into criteria perceived to be a substantial risk. There was also a dominant perception that employees inherit some level of organisational cyber-risks by being employed or associated with the financial services environment. Most of the social influence cyber-risks, such as cyberbullying or cyberstalking was; however, not evident in this study. Perceptions of health influences of cyber-risk were also established not to be top of mind for employees.

This finding adds to the cyber-risk literature in that there are distinct lenses through which individuals perceive cyber-risks encountered by themselves and their perceived individual risks were privacy and financially oriented, which aligned with the literature (Irshad & Soomro, 2018; Shahria et al., 2020), whereas perceived organisational cyber-risks were more oriented to customer privacy compromise and not much on the financial side. The lack of financial risk to the organisation is a new insight that requires further exploration to grow the literature further. Concerning perception of the vulnerability of the cyber-risk, there was alignment in that while everyone with a cyber presence or a dependency on cyber-enabled resources, has vulnerability to cyber-risk (Burton et al., 2022; Caldarulo et

al., 2022), older generations and those not trained on cybersecurity, such as the youth, have higher cyber-risk (Mishna et al., 2009; Van Schaik et al., 2017).

6.1.2 Cybersecurity awareness and training

Literature has pointed out that cyber-risk perceptions were formed based on information available to the person about the severity of the threat and their vulnerability to such threat (Van Schaik et al., 2017). Availability of information about the potential risk could be from diverse sources, such as previous exposure to cyberattacks, cybersecurity awareness and training and job types that contribute to those perceptions (Aloul, 2012; Gillam & Foster, 2020; Van Schaik et al., 2017). The role of cybersecurity awareness and training in influencing threat appraisal and coping appraisal and, by implication, risk perception was assessed in the literature (Li et al., 2019).

Beyond informing people of cyber threats and vulnerabilities, cybersecurity training also teaches how to reduce one's vulnerabilities to cyber threats (Li et al., 2019; Mou et al., 2022). Availability and awareness of information about the risk (i.e., threat appraisal) and the formed self-efficacy to defend against such risk (i.e., coping appraisal) were observed to shape how an individual would formulate or amend the risk perception (Gillam & Foster, 2020; Van Schaik et al., 2017). In cybersecurity training, people are informed of things known to reduce cyber-risks.

These options are using various tactics, such as the use of strong, unique passwords, multifactor authentication, or being cautious when dealing with emails, verifying the source of the email between replying to it, downloading its attachments, or clicking on the links in the email (Van Schaik et al., 2017). People however, have various awareness levels, such as training, education, and skills, on the subject of cybersecurity (Siponen, 2000). The implication is, therefore, that each person will have their unique perception of cyber-risk provided they are informed and trained at various levels on cybersecurity.

The study findings were that not all organisations in South African financial services have the same level of cybersecurity awareness and training programmes. While the majority came from an organisation with high maturity cybersecurity awareness and training programmes participants, where organisations employ mandatory training and periodic, structured awareness communications, there were two that came from organisations with

only periodic structured communications with no training. Two participants indicated that they had a low maturity cybersecurity awareness and training programme where their communications were ad-hoc. They lacked formal employee training. Employees also possessed various levels of awareness and training about cybersecurity.

While none had suffered a cyber breach, some participants had proximity to people that had fallen victim to cybercrime before. There was no evidence from the study that these proximity incidents have changed their cyber-risk perceptions. There was; however, evidence that participants that had technical and risk backgrounds had higher perceptions of individual and organisational cyber-risks than those coming from non-technical areas of the business, such as marketing and sales, legal, finance and operations.

This finding confirms that cyber-risk information availability can be built through cybersecurity awareness and training and the type of roles that people perform (Gillam & Foster, 2020; Van Schaik et al., 2017). Because none were a victim of cybercrime, the part of the literature that posits information availability can be built through prior experiences of cybercrime could not be assessed (Van Schaik et al., 2017).

6.1.3 Conclusion on Proposition 1

This proposition was intended to assess the existence of the relationship between the maturity of cybersecurity awareness and training that employees are exposed to the level of cyber-risk perceptions, with an expectation that where employees have exposure to higher cybersecurity awareness and training programmes, they will also have higher cyber-risk perceptions. The findings confirmed a relationship between high-maturity cybersecurity awareness and training with cyber-risk from the organisation's perspective, although the perceived risks were not according to the literature. From the individual cyber-risk perspective, cyber-risk perceptions were inconsistent among those with a similar levels of cybersecurity awareness exposure, with clear distinguishment observed from those working in technology and risk space.

Findings in this proposition add to the literature in that cyber-risk perceptions can vary based on the contexts, such as an individual can have a high organisational cyber-risk while having either similar or various perceptions when it comes to their personal side. Risk perceptions in the employee capacity were related to the participants' association

with the employer and their proximity to the resources perceived to be of interest and value to cybercriminals, such as data or the ability to transact. This association was not observed in the literature before, and therefore, this study adds to the literature by emphasising this relationship, which can be explored further and empirically assessed in future studies.

An additional contribution to the literature from the findings was a possible feedback loop emphasised between cybersecurity awareness and training and cyber-risk perceptions. It was established that once cyber-risk perceptions are formulated, cybersecurity awareness and training are then perceived as a risk countermeasure to reduce risk exposure. This phenomenon was not directed from the literature.

6.2 Proposition 2: Individual cyber-risk perception functions as a lever for protective cyber behaviour in the workplace

In Section 6.1 above, cyber-risks were described from an individual and organisational perspectives. In this section, protective cyber behaviour in the workplace was described, and findings from the study on this construct were synthesised against the literature and conclusion drawn. In the conclusion of the proposition, the relationship between individual cyber-risk perceptions and protective cyber behaviour was then analysed and presented to close off this section.

6.2.1 Protective cyber behaviours

It was understood from the literature the theories, such as PMT and the risk compensation theory, posit, that protection decision-making in a perceived risk situation is a cost-benefit analysis (Van Schaik et al., 2017). In this cost-benefit analysis, such as the response cost construct of the PMT, when encountered with decision-making, response options were weighed against each other, and the most beneficial one in that scenario would be selected (Conner & Norman, 2005; Van Schaik et al., 2017).

The outcome of threat appraisals is perceived threat severity and vulnerability, such as risk perception, which has been explored in Section 6.1 above. In the coping appraisal, response efficacy, self-efficacy and response cost are considered in the final phases of protective action decision-making (Conner & Norman, 2005). The coping appraisal was established to play a bigger role in determining whether a person will adopt protective

behaviour (Mou et al., 2022). Of the three components of coping appraisals, literature has indicated that self-efficacy has the most positive influence on the induced intention and motivation to execute protective behaviour (Li et al., 2019; Mou et al., 2022; Warkentin et al., 2016; van Bavel et al., 2019). Response cost, in this case, particularly in the organisational context, is more than the monetary value but includes other modalities, such as effort and time (Mou et al., 2022).

The literature described protective cyber behaviours, also known as cyber hygiene behaviours, as good practices that, when conducted well, will improve the cybersecurity posture of the organisation or an individual and, therefore, reduce their cyber risk (Cain et al., 2018; Vishwanath et al., 2020; Witsenboer et al., 2022). Protective cyber behaviours practised by employees can protect the employees and the organisations they work for from cyber compromise by cybercriminals and insider threats (Zimmermann & Renaud, 2019).

It is contended that people will practice a protective cyber behaviour if they can carry it out, such as they have self-efficacy and they also perceive that such action or behaviour will benefit them (Conner & Norman, 2005). While there is no globally acceptable taxonomy of protective cyber protective behaviour (Cain et al., 2018), the five domains, as presented by Vishwanath et al. (2020), summarise protective cyber behaviour. The domains as adopted from the cyber hygiene inventory (CHI) model are: 1) information storage and device hygiene, 2) network transmission hygiene, 3) social media hygiene, 4) authentication and credential hygiene, and 5) email and messaging hygiene (Vishwanath et al., 2020). Protective cyber behaviours vary in technical intensity and effort. People with no technical background and, by implication, low self-efficacy in protective cyber behaviours, technical in nature, would not carry them such protective cyber behaviours out (Cain et al., 2018).

The findings of the study indicated there are varied protective cyber behaviours then categorised into three categories, such as 1) generic behaviours, 2) specific and non-technical behaviours, and 3) specific and technical behaviours. These behaviours vary not only in specificity and technicality but in cost or effort. Considering those daily business operations are under constant cyber-risks, in the frequently cyber protective behaviour decision-making, participants only considered those options they believe would have a

positive influence on their situation, and they also had self-efficacy to conduct. When self-efficacy was present or not required, as in the case of following the defined process according to company policy, response cost was considered, and some remarked that it was mentioned when it was considered too high or an inhibitor. For example, Participant 6 shared that they have used their corporate identity for non-work-related matters when forced by the service provider not to use public email addresses. They understand this is risky behaviour from the organisational cybersecurity perspective, but their perceived cost of creating a non-public email address is observed at a much higher cost than the expected benefit.

The lack of these technical protective behaviours by people without a technical background can be contended to low self-efficacy by those people that do not engage in these behaviours. For example, backup creation was also only remarked by Participants 4 and 7 from risk and audit and cybersecurity, respectively. Similarly, system updates—a control measure of closing system vulnerabilities, were only cited by Participants 7 and 9, who are in cybersecurity and IT governance areas, respectively.

Participant 3 shared that they sometimes reuse their passwords citing that the burden of memorising numerous passwords and its perceived risk was perceived to be too lower than the benefit of reusing the passwords across multiple service platforms. Here, it can be deduced that the risky cyber behaviour was practised because the perceived cost of practising comparable cyber behaviours was considered to have excessive cost concerning effort. Participant 14 shared this same challenge as Participant 4, and they employed other mitigations, such as slightly altering the password each time and when they cannot remember the password later, they resort to using password self-service reset. This participant, however, shared that this and all other security measures or protective cyber behaviours they practice were daunting, suggesting that a perceived response cost concerning effort.

It was established that participants had reasonable levels of self-efficacy on non-technical protective cyber behaviours. In contrast, technical protective cyber behaviours, such as setting up malware protection device and running routine scans, was only evident in those participants that came from either technology or risk and audit areas. Participants that had self-efficacy practised them mostly in their personal capacities, with only one participant

sharing that they perform periodic malware scans on their work device.

Another element that seemed to be associated with protective cyber behaviour over and above the constructs of PMT discussed above and was not investigated during the literature review is personality. Two participants mentioned paranoia who self-reported consistent and broad protective cyber behaviours. This observation further explores how personalities affect cyber-risk perceptions and resultant behaviours.

These findings confirm the literature concerning the role played by self-efficacy towards cyber protection behaviour, where some observed that behaviours technical in nature were only considered and practised by those with self-efficacy in them. Findings also confirmed that response is also considered in the protective cyber behaviour decision-making and higher cost, which was mostly as required effort and the time required to either explicitly conduct a protective cyber action or to follow the defined organisational process was a determinant of the cyber behaviour decision. The findings also add to the literature in that a new dimension was observed as a possible determinant of protective cyber behaviour.

6.2.2 Conclusion of Proposition 2

The findings add to the literature by bringing in context-based risk appetite elements in addition to individual cyber-risk perception and response appraisal to the shaping of protective cyber behaviours. Participants of this study had variability in their perceptions of individual cyber-risks, with some even identifying as paranoid about cyber-risk, whereas others shared that they had disregarded that they may fall victim to cybercrime before. As for protective cyber behaviours, participants self-reported practising protective cyber behaviours; however, with some deviations in certain instances.

Protective cyber behaviours were not mutually exclusive to risky cyber behaviours. Even once a cognitive awareness of an individual cyber-risk was created, and a perception was formed, cyber behavioural decisions seemed to be context based. One person could take protective cyber behaviour in one scenario and take a risky one in another. The reason behind this context-based protective cyber behaviour decision once self-efficacy and response efficacy are developed can be attributed to the perceived net cost of that decision in that provided circumstance.

6.3 Proposition 3: Organisational cyber-risk perception does not directly shape individual protective cyber behaviour

This proposition is closely related to Proposition 2 above, with the difference in the perceived risk setting, with this one being organisational, compared to individual cyber-risk perception. In this section, organisational cyber-risk was expanded further from what was described in Section 6.1 above, and study findings were then synthesised against the organisational cyber-risk literature. In conclusion, the relationship between organisational cyber-risk perceptions and protective cyber behaviour is analysed and presented.

6.3.1 Organisational cyber-risk perceptions

Literature and industry researchers indicate that the risk encountered by organisations is increasing and not showing any signs of slowing down (Lee, 2021). These increases are attributed to several elements, such as a persistently upward trend in Internet use driven by digital transformations, improving technologies, such as artificial intelligence and other dynamics, such as remote workforce, third-party dependencies, Internet of things, adoption of BYOD, to name a few (Almarhabi et al., 2022; Curran, 2020; Eisenbach et al., 2021; Kamiya et al., 2021; Kumar et al., 2022; Tosun, 2021; Lee, 2021). The interconnectedness nature of today's ecosystem means that influence cyber breaches and incidents have more systemic influence (Burton et al., 2022; Caldarulo et al., 2022; Eisenbach et al., 2021).

From the threat actor perspective, it was established from the literature that various types of cyber threat actors differ in motivation, experience and access to financial resources from innocent internal users to organised, state-sponsored cybercriminals experienced and resourced to conduct their missions (Johnston et al., 2019; Chng et al., 2022; Warkentin et al., 2016). While several cybercriminals have financial motivations, there are those with non-financial motivations, such as curiosity (script kiddies), espionage and political motivations (Chng et al., 2022).

Findings from the study confirm the literature in that there are a high and increasing cyber-risk encountering organisations today. The systemic influence of the perceived organisational cyber-risk was also observed from the findings, particularly from the customer privacy perspective. While service disruptions were little pronounced from the

findings, the high severity and systemic influence elements were aligned with the literature. From the threats causing the risk, the study findings had strong perceptions that these are financially motivated and political motivations were not perceived to be the driver of cybercrime in organisations. The findings depicted the perceptions of high organisational cyber-risk. Organisational cyber-risk perceptions were deduced from these elements: 1) inherent risk of providing Internet-based service, 2) type of valuable data that financial organisations keep and use, 3) increasing information and technology complexities, and 4) insufficient cyber-risk mitigations.

6.3.2 Conclusion on Proposition 3

The findings in this proposition confirm the literature concerning the relationship between perceived organisational cyber-risk and the resultant protective cyber behaviours, which have emphasised the distance between cyber-risk encountered by organisations and the motivation to take protective behaviours to counter such risk (Mou et al., 2022). This phenomenon was the base of criticisms against the adoption of using the anchoring theory of this study in the cybersecurity human behaviour domain (Vishwanath et al., 2020). It was further established that participants separated themselves from those people in the organisation prone to be targeted for cybercrime.

They did not exhibit the characteristics associated with high-risk personnel, such as being in the same job for too long, not being exposed to cybersecurity training, being of an older generation or younger, and being too open and public on social media. This observation suggests that employees do not consider themselves as the possible weakest link, as it is evident from the literature (Abraham & Chengalur-Smith, 2010; Lee, 2021; Zimmermann & Renaud, 2019), which implies there is the distance between themselves and the organisational cyber-risk and the role they play in countering this risk.

Despite most participants having represented a high perception of organisational risk, some confessed to practising risky cyber behaviours despite this cognitive awareness of the risk and being trained on cybersecurity, particularly in the organisational context. Even employees with high self-efficacy in technical protective behaviours, the responsibility for technical security controls, such as ensuring that malware is running on their work device, sat with IT teams, and as end-users, they remove themselves from these protective cyber behaviours. This proposition, therefore, has been confirmed.

6.4 Closing

Protective cyber behaviours were not mutually exclusive to risky cyber behaviours. Once a cognitive awareness of the risk is created and perception is formed through awareness and training or due to the nature of their job, users' cyber behavioural decisions were context-based. One person could take protective cyber behaviour in one scenario and take a risky one in another.

Hinderances, such as forgetfulness and time-pressures, were cited as some contributors to inconsistencies in the practice of protective cyber behaviours, such as the reuse of passwords across multiple platforms or writing passwords down. Furthermore, some employees observed to have views that some technical cybersecurity controls were obstructive and not well communicated nor designed with an understanding of the business processes and needs that have also confessed to having bypassed security controls. In this context, bypassing security controls was also observed as risky cyber behaviour. These elements that shape cyber behaviour can be mapped back to the PMT model where hindrances mentioned above and perceptions of obscurity in security controls is response cost; poor communication on and the resulting lack of understanding on security controls aligns to the response efficacy subjects were not efficient on the security controls. What became evident in this study was that response efficacy and cost-efficacy were context-based and could change based on what is perceived to be at stake in that point in time.

It was also observed for some employees, when they are faced with situations that there are hinderances to protective cyber heaviours due to effort or other hinderances outlined above, they would apply further measures to counter these hindrances, such as making use of self-service password reset to avoid not using the same password across various platforms or writing the passwords down. Examples of this practice was observed with a participant that reported high perceptions of individual and organisational cyber-risk and self-identified as paranoid, which suggests a low appetite for risk, for example participants 9 and participant 14. Both these participants self-identified as paranoid.

In contrast, another participant also had high individual and organisational cyber-risk perception but reflected to be "not overly cautious", and they had a less involved approach to cyber behaviour. It can be concluded that risk appetite cannot hold a function in shaping

cyber behaviours. From these, it could be concluded that high sensitivity or personality personality results in low risk appetite, which results in more protective cyber behaviours.

There was also evidence of a uni-directional domain spillage of cyber-risk between the employer and employee that emerged in the data analysis. For example, participants expressed that they believe that their association with their employer or their specific roles in their organisation made them an attractive target for cyberattacks.

6.4.1 Discussions against the originally proposed model

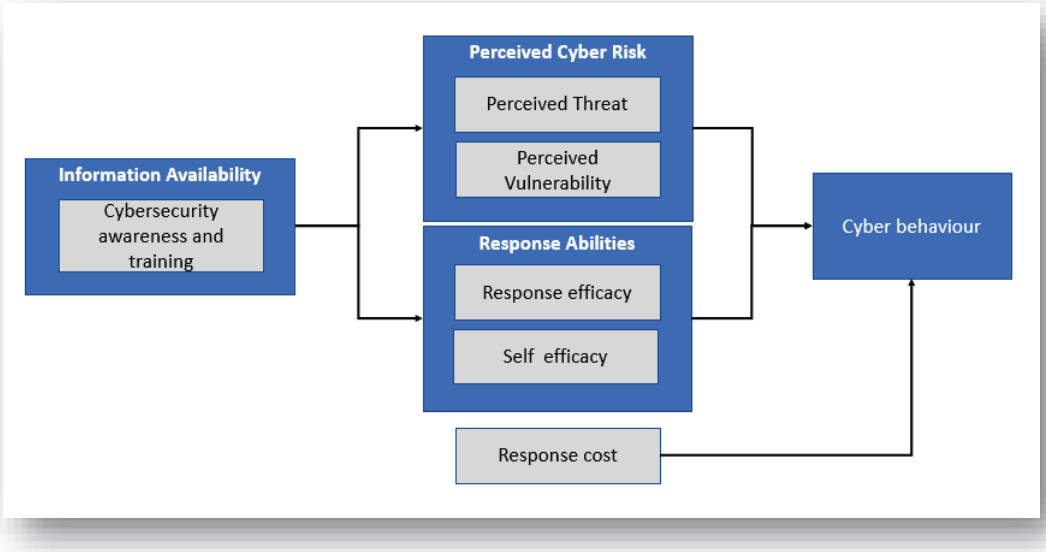


Figure 23: Cyber behaviour model

Some indicated that where the perceived individual cyber-risk is relatively high, employees would engage the cybersecurity awareness and training more and aim to learn to stay abreast of the current risks. They learn how to be armed on how to respond to them. Individual cyber-risk perception shapes how people relate and engages with the awareness and training on the subject to understand how they can minimise their residual risk exposure. This observation suggested a feedback loop between cybersecurity awareness and training construct and individual cyber-risk perceptions.

A uni-directional cyber-risk domain spillage between the employees and their emerged in the data analysis even though it was not indicated during the initial literature review in

Chapter 2. For example, participants expressed that they believe that they make attractive cybercrime targets by them being employed by organisations in financial services. Personality also emerged as a contributing element to cyber-risk perceptions and cyber behaviours.

6.4.2 Revised model

After the data synthesis was conducted against the literature, the model defined in Chapter 2 was revised to include the insights that emerged from the data. First, the feedback loop between perceived cyber-risk and cybersecurity awareness and training is depicted in the revised model. Second, the unidirectional cyber-risk domain spillage observed from the data analysis is also depicted. Third, the function of personalities in creating a perception of the response cost, as indicated in Proposition 3, is also depicted in the revised model.

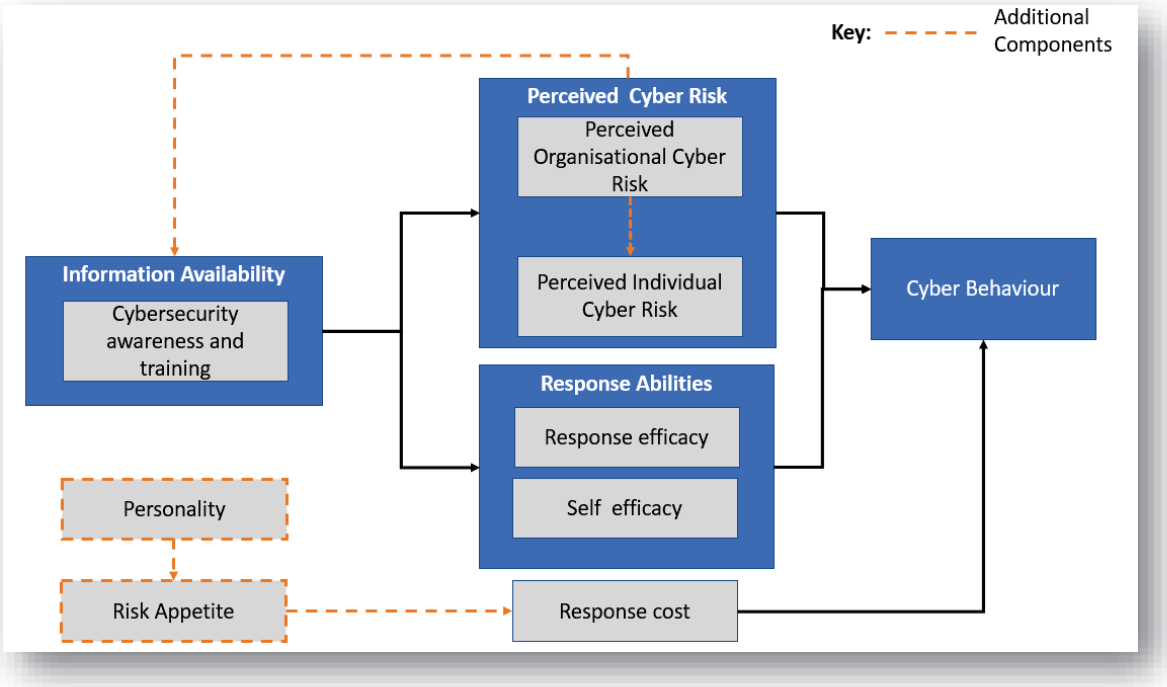


Figure 24: Revised cyber behaviour model

CHAPTER 7: CONCLUSIONS AND RECOMMENDATIONS

7.1 Principal conclusions

This study's findings align with prior studies that emphasised low motivations and intentions to adopt protective behaviours when the perceived influence is the distance before the subject, as in employees concerning perceived organisational cyber-risks (Mou et al., 2022). This study confirmed that employee's cyber-risk perceptions shape cyber protective behaviours, particularly when the person is confident that such protective action behaviour has a positive influence on reducing the cyber-risk (i.e., have response efficacy). They can also conduct the action (self-efficacy) with reasonable effort (response cost).

It was; however, evident that the relationship between individual cyber-risk perceptions and cyber behaviour is context-based and not binary in that even though the person may have response efficacy and self-efficacy to conduct a protective cyber action, results of the cost determination may vary from case to case. This fluid and dynamic nature of perceived cost may be the potential reason some researchers in the past left the element of perceived response cost when applying Protection Motivation Theory (PMT) in cybersecurity human behaviour (Chen & Zahedi, 2016). From the employee perspective, the cost is mostly considered concerning effort and time required to take protective action.

Such action would reduce the risk, such as input cost, according to the previous studies that did not find the cost to be playing a role in shaping cyber behaviours in the working environment (Mou et al., 2022; van Bavel et al., 2019). The potential individual risk implications include lost productivity time owing to downtime, loss of work or personal data, embarrassment, reputational risk, identity theft, job loss, financial loss, physical harm and, in the case of top management, imprisonment if the gross the cyber breach or incident is associated with gross negligence from organisational leadership (Ogbanufe et al., 2021)

The positive role of cybersecurity awareness and training in building and shaping individual and organisational cyber-risk perceptions has been confirmed, which also aligns with prior studies (Chandarman & Van Niekerk, 2017; D'Arcy et al., 2009; Dawson & Thomson, 2018; Pollini et al., 2021; Öğütçü et al., 2016; Siponen, 2000). Personalities

were also established to play a role in defining cyber-risk perceptions and cyber behaviours. Some also observed that once people are cognizant of their individual cyber-risk exposure, they engage in cyber-security awareness communications and training with the added purpose of arming themselves with knowledge of what types of risks to leveraged by cybercriminals and how they can protect themselves against those tactics, such as improve their self-efficacy.

Based on these insights, business leaders and cybersecurity professionals can craft cybersecurity awareness and training programmes to influence individual cyber-risk perceptions and create a link between the individual risk and the desired protective behaviour within the work context. This provides an answer to the main research question of this study on how organisational leaders and cybersecurity awareness and training progress can be aimed to shape employee protective cyber behaviours.

7.2 Theoretical contribution and implications

This study contributed to the cyber-risk and cybersecurity theory by exploring cyber-risk from the individual and organisational contexts and emphasising possible ways these cross-domain of cyber-risk considerations can be beneficial in instilling protective cyber behaviours among employees. Provided that employees have distance between themselves and the organisational cyber-risk, causing lower motivation to adopt protective cyber behaviours voluntarily, there is an opportunity to leverage the closeness of perceived individual cyber-risk when encouraging their employees to adopt protective cyber behaviours voluntarily.

Implications to organisational leaders and those responsible for designing cybersecurity awareness and training in their organisations is to design these programmes in a manner that increases focus on the individual needs of the employees, and build their skills on how to reduce their own individual cyber-risks understanding that such built behaviours will spill over into the work domain. This is a new approach compared to the common approach of focusing communication and training on organisational risk mitigations and not individual ones (Li et al., 2019; Liu et al., 2020).

Protective cyber behaviour can be reduced by reducing the distance between users and

influence from potential cyber breaches or incidents. While BYOD was strongly perceived as a risk-increasing practice by participants of this study, the researcher presents that BYOD, as a form of autonomy, should be considered by organisational leadership and cybersecurity policymakers for its potential to increase the influence cost for employees if they are compromised. This is suggested because it would be their personal machine, with their personal data also at risk, and as such, they would be more inclined to practice technical and non-technical protective cyber behaviours.

Provided that people also have varying levels of cybersecurity knowledge and self-efficacy protective cyber behaviours and have diverse personalities. By implication, diverse attitudes and perceptions on cyber-risks and interventions that organisations have implemented to counter such risks, designers of cybersecurity awareness and training programmes should consider a more individual approach not only progressive in skill level but also offered in various delivery channels and allow employees to be enrolled into the training that will be valuable to them, concerning either increasing their knowledge on the subject while keeping abreast as opposed to generic and repeated content delivered to employees. This could create interest in those not working in cybersecurity to shift into this domain with skill shortages. According to the Cybercrime Magazine, there will be 3. 5 million vacant cybersecurity roles by 2025 in the United States alone owing to skill shortage (Morgan, 2019).

7.3 Limitations of the research

This study has not been without limitations. In this section, limitations are discussed, and where possible, mitigations applied are also articulated.

- Cyber-risks are vast, and there is a risk that participants may either not understand these risks or provide their insights based on a single type of cyber-risk. During the interview process, the researcher sought to understand how each participant thought of cyber-risks and shared a description considered overarching and holistic to allow a mutual understanding.
- The study took an open approach to cyber behaviours instead of focusing on specific behaviours. While this was conducted to avoid being too specific, the risk of the

approach taken in the current study is that participants may not have thought of certain actions as protective behaviours.

- This study was conducted with participants within South Africa. Inference, generalisation, or applications of the results in various geographic regions may be impractical. It is expected that the data may contain geographical biases specific to South Africa. Further studies should be conducted in other geographic regions and compared to the study outcomes.
- From the methodology perspective, this research aimed to explore the relationship between constructs using a qualitative approach rather than a qualitative approach as the study aimed to obtain detailed insights to build on existing theories in this domain rather than to assess already established theories empirically. These relationships will require further longitudinal empirical testing for people with no exposure to cybersecurity training and two groups where one is exposed to cybersecurity awareness and training that have messages focusing on organisational cyber-risks with the other groups exposed to messages focused on individual cyber-risks methods in future studies.
- The purposive sampling method is subject to researcher biases as the onus is on the researcher to interview participants from the qualifying population.
- The sample in this study included participants with varying levels of exposure and proximity to the cybersecurity domain, which may cause non-consistency in the results. Future studies should aim to set the samples into more homogenous groups from the job type perspective.
- Attributable to the large population, this research focused on participants from legal, IT, finance, operations, marketing, and sale and risk and audit, to obtain representative views from cyber-risk perceptions and other related insights. While other studies established these among crucial business divisions to consider in organisations when studying employees, this may still be open to the risk of the study being representative.
- The interviews were conducted over a teleconference medium, and video was not enabled in all the interviews either owing to participants' confidentiality concerns or poor network connectivity conditions during the interviews. This added more limitations to the researcher's ability to observe nonverbal cues during the interview. There is a

risk that participants may have had split attention and focus during the interview.

- cybersecurity domain is a sensitive topic, and participants may be uncomfortable freely sharing their observations. To mitigate this, the interviews were conducted individually, and each participant was provided with an affirmation that their confidentiality and that they were participating in their capacity and not representing the organisations where they work.

7.4 Suggestions for future research

It was evident from this study that levels of self-efficacy to conduct actions or behaviours that are technically inclined vary among employees, but there is no universally acceptable categorisation of protective cyber behaviours between technical and non-technical. While this study attempted to categorise them into technical and non-technical categories based on the collected data, more studies focused on this objective need to be conducted in future to define a conceptual model that can reduce the room for subjectivity in future studies on cybersecurity human behaviour. Such conceptual model of protective behaviours categories can be mapped to levels of cybersecurity training which could then allow employees to enrol for those training that will be challenging to them, keep building, and improve their self-efficacy where they need to build more rather than repeating the same training repeatedly.

Future research can also explore the function of personalities in cyber behaviours. Personalities emerged in the current study, but further studies would provide valuable input to researchers, policymakers, and cybersecurity professionals in their cybersecurity program. Results of such a study could also be input into the cyber training and awareness programmes where for example, people can be engaged and trained in manners that would be best receptive to them based on their personalities.

While the relationship between personal closeness to the perceived cyber-risk and resultant cyber behaviours was included in this study (Propositions 2 and 3), future research could empirically test this phenomenon. Last, with healthcare being among the industries that have observed an increase in cyber breaches and incidents in the last few years, and the influence of such breaches is close to life and death, researchers should

explore how the study findings would compare to this industry, especially in the South African context known to be collectivism and ubuntu and not much of an individualist approach.

REFERENCES

Ablon, L. (2018). The motivations of cyber threat actors and their use and monetization of stolen data. In *Rand*. https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT490/RAND_CT490.pdf

Abraham, S., & Chengalur-Smith, I. (2010). An overview of social engineering malware: Trends, tactics, and implications. *Technology in Society*, *32*(3), 183–196. https://doi.org/10.1016/j.techsoc.2010.07.001

Aldasoro, I., Gambacorta, L., Giudici, P., & Leach, T. (2022). The drivers of cyber-risk. *Journal of Financial Stability*, *60*, 100989. https://doi.org/10.1016/j.jfs.2022.100989

Alharahsheh, H., & Pius, A. (2020). A Review of key paradigms: positivism VS interpretivism. *Global Academic Journal of Humanities and Social Sciences*, *2*(3), 39–43. https://doi.org/10.36348/gajhss.2020.v02i03.001

Almarhabi, K., Bahaddad, A., & Mohammed Alghamdi, A. (2022). Security management of BYOD and cloud environment in Saudi Arabia. *Alexandria Engineering Journal*, *63*. https://doi.org/10.1016/j.aej.2022.07.031

Aloul, F. A. (2012). The need for effective information security awareness. *Journal of Advances in Information Technology*, 3(3). https://doi.org/10.4304/jait.3.3.176-183Alsharnouby, M., Alaca, F., & Chiasson, S. (2015). Why phishing still works: User strategies for combating phishing attacks. *International Journal of Human-Computer Studies*, *82*, 69–82. https://doi.org/10.1016/j.ijhcs.2015.05.005

Antonescu, M., & Birău, R. (2015). Financial and non-financial implications of cybercrimes in emerging countries. *Procedia Economics and Finance*, *32*, 618–621. https://doi.org/10.1016/s2212-5671(15)01440-9

Asatiani, A., Penttinen, E., & Kumar, A. (2019). Uncovering the nature of the relationship between outsourcing motivations and the degree of outsourcing: An empirical study on Finnish small and medium-sized enterprises. *Journal of Information Technology*, *34*(1), 39–58. https://doi.org/10.1177/0268396218816255

Babcicky, P., & Seebauer, S. (2019). Unpacking protection motivation theory: Evidence for a separate protective and non-protective route in private flood mitigation behavior. *Journal of Risk Research*, 22(12), 1503–1521.

https://doi.org/10.1080/13669877.2018.1485175

Bacchus, A. (2020, March 2). Teams, Zoom, Slack, and more: These are the top teleconference solutions to consider in the wake of the Coronavirus outbreak. *OnMSFT.* https://www.onmsft.com/feature/teams-zoom-slack-and-more-these-are-the-top-teleconference-solutions-to-consider-in-the-wake-of-the-coronavirus-outbreak

Baig, A., Hall, B., Jenkins, P., Lamarre, E., & McCarthy, B. (n.d.). *Digital adoption through COVID-19 and beyond | McKinsey*. www.mckinsey.com. https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-covid-19-recovery-will-be-digital-a-plan-for-the-first-90-days

Bendovschi, A. (2015). Cyber-Attacks – Trends, patterns and security countermeasures. *Procedia Economics and Finance*, *28*(28), 24–31. https://doi.org/10.1016/s2212-5671(15)01077-1

Boss, S. R., Galletta, D. F., 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

Bressler, M., & Bressler, L. (2014). Protecting your company's intellectual property assets from cyber-espionage. *Journal of Legal, Ethical and Regulatory Issues*, *17*(1).

Brewster, T. (2020, June 3). *Huge cyberattacks attempt to silence black rights movement with DDoS attacks. Forbes*. https://www.forbes.com/sites/thomasbrewster/2020/06/03/huge-cyber-attacks-attempt-to-silence-black-rights-movement-with-ddos-attacks/?sh=300f0800742b

Bronk, C. (2015). Two securities: How contemporary cyber geopolitics impacts critical infrastructure protection. *International Journal of Critical Infrastructure Protection*, *8*, 24–26. https://doi.org/10.1016/j.ijcip.2014.12.001

Burns, A. J., Posey, C., Roberts, T. L., & Benjamin Lowry, P. (2017). Examining the relationship of organizational insiders' psychological capital with information security threat and coping appraisals. C*omputers in Human Behavior*, *68*, 190–209. https://doi.org/10.1016/j.chb.2016.11.018

Burton, A., Cooper, C., Dar, A., Mathews, L., & Tripathi, K. (2022). Exploring how, why and in what contexts older adults are at risk of financial cybercrime victimisation: A

realist review. *Experimental Gerontology*, *159*, 111678. https://doi.org/10.1016/j.exger.2021.111678

Cain, A. A., Edwards, M. E., & Still, J. D. (2018). An exploratory study of cyber hygiene behaviors and knowledge. *Journal of Information Security and Applications*, *42*, 36–45. https://doi.org/10.1016/j.jisa.2018.08.002

Caldarulo, M., Welch, E. W., & Feeney, M. K. (2022). Determinants of cyber-incidents among small and medium US cities. *Government Information Quarterly*, *39*, 101703. https://doi.org/10.1016/j.giq.2022.101703

Capitec integrated annual report 2021. (2021). https://www.capitecbank.co.za/globalassets/pages/investor-relations/financial-results/2021/annual-report/integrated_annual_report_2021.pdf

Carpenter, D., Young, D. K., Barrett, P., & McLeod, A. J. (2019). Refining technology threat avoidance theory. C*ommunications of the Association for Information Systems*, *44*, 380–407. https://doi.org/10.17705/1cais.04422

Chandarman, R., & Van Niekerk, B. (2017). Students' cybersecurity awareness at a private tertiary educational institution. *The African Journal of Information and Communication*, 20, 133–155. https://doi.org/10.23962/10539/23572

Chen, Y., & Zahedi, F. M. (2016). Individuals' internet security perceptions and behaviors: polycontextual contrasts between the United States and China. *MIS Quarterly*, 40(1), 205–222. https://doi.org/10.25300/misq/2016/40.1.09Cheung, K.-F., Bell, M. G. H., & Bhattacharjya, J. (2021). Cybersecurity in logistics and supply chain management: An overview and future research directions. *Transportation Research Part E: Logistics and Transportation Review*, *146*, 102217. https://doi.org/10.1016/j.tre.2020.102217

Chng, S., Lu, H. Y., Kumar, A., & Yau, D. (2022). Hacker types, motivations and strategies: A comprehensive framework. C*omputers in Human Behavior Reports*, *5*, 100167. https://doi.org/10.1016/j.chbr.2022.100167

Cho, J., & Trent, A. (2006). Validity in qualitative research revisited. *Qualitative Research*, *6*(3), 319–340. https://doi.org/10.1177/1468794106065006

Choudhury, S. (2020, August 10). C*ISOs consider cyber threats as their businesses' risks*. ITSecurityWire. https://itsecuritywire.com/featured/cisos-consider-cyber-threats-as-their-businesses-risks/

Clough, J. (2011). Data theft? Cybercrime and the increasing criminalization of access to data. C*riminal Law Forum*, *22*(1-2), 145–170. https://doi.org/10.1007/s10609-011-9133-5

Conner, M., & Norman, P. (2005). *Predicting health behaviour*. Open University Press. https://iums.ac.ir/files/hshe-soh/files/predicting_Health_beh_avior(1).pdf#page=18

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. C*omputers & Security*, *32*, 90–101. https://doi.org/10.1016/j.cose.2012.09.010

Curran, K. (2020). Cyber security and the remote workforce. C*omputer Fraud & Security*, *2020*(6), 11–12. https://doi.org/10.1016/s1361-3723(20)30063-4

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach*. Information Systems Research*, 20(1), 79–98. https://doi.org/10.1287/isre.1070.0160

Dawson, J., & Thomson, R. (2018). The future cybersecurity workforce: Going beyond technical skills for successful cyber performance. *Frontiers in Psychology*, 9. https://doi.org/10.3389/fpsyg.2018.00744

Deibert, R., & Rohozinski, R. (2009). Tracking GhostNet: Investigating a cyber espionage network. In *Tracking GhostNet*. Information Warfare Monitor. https://ora.ox.ac.uk/objects/uuid:6d1260fd-b8ee-4a11-8a5f-e7708d543651/download_file?safe_filename=Gh0stNet.pdf&file_format=application%2Fpdf&type_of_work=Report

Deloitte. (2020, January 9). *91% of all cyber attacks begin with a phishing email to an unexpected victim*. Deloitte Malaysia. https://www2.deloitte.com/my/en/pages/risk/articles/91-percent-of-all-cyber-attacks-begin-with-a-phishing-email-to-an-unexpected-victim.html

Desjardins, J. (2019, March 13). *What Happens in an internet minute in 2019?* Visual Capitalist. https://www.visualcapitalist.com/what-happens-in-an-internet-minute-in-2019/

Digital Commerce Acceleration. (2021). In *Deloite*. https://www2.deloitte.com/content/dam/Deloitte/za/Documents/strategy/za-Digital-Commerce-Acceleration-2021-Digital.pdf

Donalds, C., & Osei-Bryson, K.-M. (2020). Cybersecurity compliance behavior: Exploring

the influences of individual decision style and other antecedents. *International Journal of Information Management*, *51*, 102056. https://doi.org/10.1016/j.ijinfomgt.2019.102056

Dredge, R., Gleeson, J., & de la Piedad Garcia, X. (2014). Cyberbullying in social networking sites: An adolescent victim's perspective. C*omputers in Human Behavior*, *36*, 13–20. https://doi.org/10.1016/j.chb.2014.03.026

Eisenbach, T. M., Kovner, A., & Lee, M. J. (2021). Cyber-risk and the U.S. financial system: A pre-mortem analysis. *Journal of Financial Economics*, *145*(3). https://doi.org/10.1016/j.jfineco.2021.10.007

Federal Bureau of Investigation. (2021). *Internet crime report 2021*. www.ic3.Gov. https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

Finkle, J. (2010, March 3). Google China hackers stole source code - researcher. *Reuters*. https://www.reuters.com/article/china-google-idUSN0325873820100303

Finucane, M. L., Alhakami, A., Slovic, P., & Johnson, S. M. (2000). The affect heuristic in judgments of risks and benefits. *Journal of Behavioral Decision Making*, *13*(1), 1–17. https://doi.org/3.0.co;2-s">10.1002/(sici)1099-0771(200001/03)13:1<1::aid-bdm333>3.0.co;2-s

Firstrand material risk factor disclosure. (2022). https://www.firstrand.co.za/media/investors/annual-reporting/firstrand-material-risk-factor-disclosure-2022.pdf

Gale, M., Bongiovanni, I., & Slapnicar, S. (2022). Governing cybersecurity from the boardroom: Challenges, drivers, and ways ahead. C*omputers & Security*, *121*, 102840. https://doi.org/10.1016/j.cose.2022.102840

Gambal, M.-J., Asatiani, A., & Kotlarsky, J. (2022). Strategic innovation through outsourcing – A theoretical review. *The Journal of Strategic Information Systems*, *31*(2), 101718. https://doi.org/10.1016/j.jsis.2022.101718

Gillam, A. R., & Foster, W. T. (2020). Factors affecting risky cybersecurity behaviors by U.S. workers: An exploratory study. C*omputers in Human Behavior*, *108*, 106319. https://doi.org/10.1016/j.chb.2020.106319

Goldkuhl, G. (2012). Pragmatism vs interpretivism in qualitative information systems research. *European Journal of Information Systems*, *21*(2), 135–146. https://doi.org/10.1057/ejis.2011.54

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

Hadlington, L. (2018). Employees attitude towards cyber security and risky online behaviors: An empirical assessment in the United Kingdom. *International Journal of Cyber Criminology*, *12*(1), 262–274. https://doi.org/10.5281/zenodo.495776

Härting, R.-C., Bühler, L., Winter, K., & Gugel, A. (2022). The threat of industrial espionage for SME in the age of digitalization. *Procedia Computer Science*, *207*, 2940–2949. https://doi.org/10.1016/j.procs.2022.09.352

Hon, W. K., & Millard, C. (2018). Banking in the cloud: Part 1 – banks' use of cloud services. C*omputer Law & Security Review*, *34*(1), 4–24. https://doi.org/10.1016/j.clsr.2017.11.005

Ikeda, S. (2022, March 23). *White house warns Russia is preparing cyber attacks against US, private Businesses Should Bolster Cyber Defenses*. CPO Magazine. https://www.cpomagazine.com/cyber-security/white-house-warns-russia-is-preparing-cyber-attacks-against-us-private-businesses-should-bolster-cyber-defenses/

Federal Bureau of Investigation. (2021). Internet Crime Report 2021. www.ic3.Gov. https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

Irshad, S., & Soomro, T. R. (2018). Identity theft and social media. *IJCSNS International Journal of Computer Science and Network Security*, *18*(1).

Jalali, M. S., Siegel, M., & Madnick, S. (2019). Decision-making and biases in cybersecurity capability development: Evidence from a simulation game experiment. *The Journal of Strategic Information Systems*, *28*(1), 66–82. https://doi.org/10.1016/j.jsis.2018.09.003

Jenik, C. (2021, July 30). *Infographic: A minute on the internet in 2021*. Statista Infographics. https://www.statista.com/chart/25443/estimated-amount-of-data-created-on-the-internet-in-one-minute/

Johnston, A. C., Warkentin, M., Dennis, A. R., & Siponen, M. (2019). Speak their language: Designing effective messages to improve employees' information security decision making. *Decision Sciences*, 50(2), 245–284. https://doi.org/10.1111/deci.12328

Johnston, & Warkentin. (2010). Fear appeals and information security behaviors: An

empirical study. *MIS Quarterly*, 34(3), 549. https://doi.org/10.2307/25750691

Kamiya, S., Kang, J.-K., Kim, J., Milidonis, A., & Stulz, R. M. (2021). Risk management, firm reputation, and the influence of successful cyberattacks on target firms. *Journal of Financial Economics*, *139*(3), 719–749. https://doi.org/10.1016/j.jfineco.2019.05.019

Karklins, L., & Dalton, D. (2012). Social networking sites and the dangers they pose to youth: Some australian findings. *Current Issues in Criminal Justice*, 24(2), 205–222. https://doi.org/10.1080/10345329.2012.12035955

Kelliher, F. (2005). Interpretivism and the pursuit of research legitimisation: An integrated approach to single case design. *Electronic Journal of Business Research Methods*, *3*(2), 123–132.

Kothe, E. J., Ling, M., North, M., Klas, A., Mullan, B. A., & Novoradovskaya, L. (2019). Protection motivation theory and pro-environmental behaviour: A systematic mapping review. *Australian Journal of Psychology*, *71*(4), 411–432. https://doi.org/10.1111/ajpy.12271

Kshetri, N. (2019). Cybercrime and cybersecurity in Africa. *Journal of Global Information Technology Management*, *22*(2), 77–81. https://doi.org/10.1080/1097198x.2019.1603527

Kumar, R., Sharma, S., Vachhani, C., & Yadav, N. (2022). What changed in the cyber-security after COVID-19? *Computers & Security*, *120*, 102821. https://doi.org/10.1016/j.cose.2022.102821

Labuschagne, A., Eloff, M., & Veerasamy, N. (2012). *The dark side of web 2.0* (pp. 237–249).

Labuschagne, H. (2022, August 18). *ID documents and contact details exposed in Vodacom fibre reseller data breach*. My Broadband. https://mybroadband.co.za/news/security/457043-id-documents-and-contact-details-exposed-in-vodacom-fibre-reseller-data-breach.html

Lauver, M. (2022, May 9). Top 5 cyber threats of Q1 2022 | Security Magazine. *Security Magazine*. https://www.securitymagazine.com/articles/97657-top-5-cyber-threats-of-q1-2022

Lai, F., Li, D., & Hsieh, C.-T. (2012). Fighting identity theft: The coping perspective. *Decision Support Systems*, *52*(2), 353–363.

https://doi.org/10.1016/j.dss.2011.09.002

Lee, I. (2021). Cybersecurity: Risk management framework and investment cost analysis. *Business Horizons*, *64*(5). https://doi.org/10.1016/j.bushor.2021.02.022

Li, J. (2018). Cyber security meets artificial intelligence: a survey. *Frontiers of Information Technology & Electronic Engineering*, *19*(12), 1462–1474. https://doi.org/10.1631/fitee.1800573

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the influence of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management*, *45*, 13–24. https://doi.org/10.1016/j.ijinfomgt.2018.10.017

Liang, H., & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems*, 11(07), 394–413. https://doi.org/10.17705/1jais.00232

Lievens, E. (2014). Bullying and sexting in social networks: Protecting minors from criminal acts or empowering minors to cope with risky behaviour? *International Journal of Law, Crime and Justice*, *42*(3), 251–270. https://doi.org/10.1016/j.ijlcj.2014.02.001

Liu, C., Wang, N., & Liang, H. (2020). Motivating information security policy compliance: The critical role of supervisor-subordinate guanxi and organizational commitment. *International Journal of Information Management*, *54*, 102152. https://doi.org/10.1016/j.ijinfomgt.2020.102152

Loughran, J. (2020, May 19). *Majority of cyber crime found to be financially motivated*. Eandt.theiet.org. https://eandt.theiet.org/content/articles/2020/05/majority-of-cyber-crime-found-to-be-financially-motivated/

McCracken, G. D. (1988). *The long interview* (Vol. 13). Sage.

Maxwell, J. A. (2013). *Qualitative research design: An interactive approach*. Sage.

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

Mishna, F., Cook, C., Saini, M., Wu, M., & MacFadden, R. (2009). Interventions for children, youth, and parents to prevent and reduce cyber abuse. *Campbell Systematic Reviews*, 5(1). https://doi.org/10.4073/csr.2009.2

Mishra, S., & Soni, D. (2020). Smishing Detector: A security model to detect smishing through SMS content analysis and URL behavior analysis. *Future Generation Computer Systems*, *108*, 803–815. https://doi.org/10.1016/j.future.2020.03.021

Monteith, S., Bauer, M., Alda, M., Geddes, J., Whybrow, P. C., & Glenn, T. (2021). Increasing cybercrime since the pandemic: concerns for psychiatry. C*urrent Psychiatry Reports*, *23*(4). https://doi.org/10.1007/s11920-021-01228-w

Monzon, L. (2021, September 22). *African bank warns of data breach after partner struck by ransomware - IT news Africa - up to date technology news, IT news, digital news, telecom news, mobile news, gadgets news, analysis and reports*. IT News Africa. https://www.itnewsafrica.com/2021/09/african-bank-warns-of-data-breach-after-partner-struck-by-ransomware/

Morgan, S. (2019, July 19). *Cybersecurity jobs report 2018-2021*. Cybercrime Magazine. https://cybersecurityventures.com/jobs/

Mou, J., Cohen, J., Bhattacherjee, A., & Kim, J. (2022). A assess of protection motivation theory in the information security literature: A meta-analytic structural. *Journal of the Association for Information Systems*, *23*(1), 196–236. https://doi.org/doi: 10.17705/1jais.00723

Mouratidis, K., & Papagiannakis, A. (2021). COVID-19, internet, and mobility: The rise of telework, telehealth, e-learning, and e-shopping. *Sustainable Cities and Society*, *74*, 103182. https://doi.org/10.1016/j.scs.2021.103182

Musetti, A., Grazia, V., Alessandra, A., Franceschini, C., Corsano, P., & Marino, C. (2022). Vulnerable narcissism and problematic social networking sites use: Focusing the lens on specific motivations for social networking sites use. *Healthcare*, *10*(9), 1719. https://doi.org/10.3390/healthcare10091719

Mutune, G. (2020, July 23). C*ybersecurity compliance requirements in 2021*. CyberExperts.com. https://cyberexperts.com/ cybersecurity-compliance/

Neuman, D., (2014). Qualitative research in educational communications and technology: a

brief introduction to principles and procedures. *Journal of Computing in Higher Education*, 26, 69–86. https://doi.org/10.1007/s12528-014-9078-x

NIST (2018). *Framework for Improving Critical Infrastructure Cybersecurity*. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

O'Kane, P., Sezer, S., & Carlin, D. (2018). Evolution of ransomware. *IET Networks*, *7*(5), 321–327. https://doi.org/10.1049/iet-net.2017.0207

O'Leary, D. E. (2019). What phishing e-mails reveal: An exploratory analysis of phishing attempts using text analyzes. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3427436

Ogbanufe, O., Kim, D. J., & Jones, M. C. (2021). Informing cybersecurity strategic commitment through top management perceptions: The role of institutional pressures. *Information & Management*, *58*(7), 103507. https://doi.org/10.1016/j.im.2021.103507

Öğütçü, G., Testik, Ö. M., & Chouseinoglou, O. (2016). Analysis of personal information security behavior and awareness. C*omputers & Security*, *56*, 83–93. https://doi.org/10.1016/j.cose.2015.10.002

Old Mutual Integrated report 2021 (pp. 8–40). (2021). https://www.oldmutual.com/v3/assets/blt566c98aeecc1c18b/bltd9a32b4b931f13b9/6261970db04465339a550c45/2021_Integrated_Report.pdf

Pienta, D., Thatcher, J. B., & Johnston, A. (2020). Protecting a whale in a sea of phish. *Journal of Information Technology*, *35*(3), 214–231. https://doi.org/10.1177/0268396220918594

Pienta, D., Thatcher, J. B., & Johnston, A. C. (2018). *A taxonomy of phishing: Attack types spanning economic, temporal, breadth, and target boundaries*. https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1018&context=wisp2018

Pollini, A., Callari, T. C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F., & Guerri, D. (2021). Leveraging human factors in cybersecurity: an integrated methodological approach. C*ognition, Technology & Work*. https://doi.org/10.1007/s10111-021-00683-y

Posey, C., Roberts, T. L., & Lowry, P. B. (2015). The influence of organizational commitment on insiders' motivation to protect organizational information assets. *Journal of Management Information Systems*, *32*(4).

South African Government. (2013). Protection of personal information act 4 of 2013 | South African government. www.gov.za. https://www.gov.za/documents/protection-personal-information-act

Provos, N., Rajab, M. A., & Mavrommatis, P. (2009). Cybercrime 2.0. C*ommunications of*

the ACM, *52*(4), 42. https://doi.org/10.1145/1498765.1498782

Quallo-Wright, M. (2022, July 5). *Preparing for the long haul: the cyber threat from Russia*. Www.ncsc.gov.uk. https://www.ncsc.gov.uk/blog-post/preparing-the-long-haul-the-cyber-threat-from-russia

Reveron, D. S., & Savage, J. E. (2020). Cybersecurity convergence: Digital human and national security. *Orbis*, 64(4), 555–570. https://doi.org/10.1016/j.orbis.2020.08.005

Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. *future internet*, *11*(4), 89. https://doi.org/10.3390/fi11040089

Saunders, M., & Lewis, P. (2018). *Doing research in business and management an essential guide to planning your project* (2nd ed.). Harlow Pearson.

Segal, E. (2022, January 5). *The 10 biggest risks and threats for businesses in 2022*. Forbes. https://www.forbes.com/sites/edwardsegal/2022/01/05/the-10-biggest-risks-and-threats-for-businesses-in-2022/?sh=5066700b366c

Shahria, M. M., Uddin, M. N., & Ahmed, M. (2020). Social media security: Identity theft prevention. *International Journal of Innovative Science and Research Technology*, 5(8), 1656–1662. https://doi.org/10.38124/ijisrt20aug762

Shenton, A. K. (2004). Strategies for ensuring trustworthiness in qualitative research projects. *Education for Information*, *22*(2), 63–75. https://doi.org/10.3233/efi-2004-22201

Sher-Lun, M., & Nicoll, S. (2020, June 6). Who is liable for an intercepted payment? *Swart*. https://www.swart.law/post.aspx?id=66

Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, *8*(1), 31–41. https://doi.org/10.1108/09685220010371394

Slapničar, S., Vuko, T., Čular, M., & Drašček, M. (2022). Effectiveness of cybersecurity audit. *International Journal of Accounting Information Systems*, *44*, 100548. https://doi.org/10.1016/j.accinf.2021.100548

Sommestad, T., Karlzén, H., & Hallberg, J. (2015). A Meta-analysis of studies on protection motivation theory and information security behaviour. *International Journal of Information Security and Privacy*, *9*(1), 26–46. https://doi.org/10.4018/ijisp.2015010102

Song, J., & Moon, Y. (2020). Security enhancement against insiders in cyber-manufacturing systems. *Procedia Manufacturing*, *48*, 864–872. https://doi.org/10.1016/j.promfg.2020.05.124

Standard Bank Group Annual Integrated Report (p. 85). (2021).

Stine, I., Rice, M., Dunlap, S., & Pecarina, J. (2017). A cyber-risk scoring system for medical devices. *International Journal of Critical Infrastructure Protection*, *19*, 32–46. https://doi.org/10.1016/j.ijcip.2017.04.001

Strupczewski, G. (2021). Defining cyber-risk. *Safety Science*, *135*, 105143. https://doi.org/10.1016/j.ssci.2020.105143

Tonn, G., Kesan, J. P., Zhang, L., & Czajkowski, J. (2019). Cyber risk and insurance for transportation infrastructure. *Transport Policy*, 79, 103–114. https://doi.org/10.1016/j.tranpol.2019.04.019

Taylor, A. (2018, March 27). *The role of compliance in cyber security*. APMG International. https://apmg-international.com/article/role-compliance-cyber-security

Tosun, O. K. (2021). Cyber-attacks and stock market activity. *International Review of Financial Analysis*, *76*, 101795. https://doi.org/10.1016/j.irfa.2021.101795

van Bavel, R., Rodríguez-Priego, N., Vila, J., & Briggs, P. (2019). Using protection motivation theory in the design of nudges to improve online security behaviour. *International Journal of Human-Computer Studies*, *123*, 29–39. https://doi.org/10.1016/j.ijhcs.2018.11.003

van de Weijer, S. G. A., Leukfeldt, R., & Bernasco, W. (2018). Determinants of reporting cybercrime: A comparison between identity theft, consumer fraud, and hacking. *European Journal of Criminology*, *16*(4), 486–508. https://doi.org/10.1177/1477370818773610

van Schaik, P., Jeske, D., Onibokun, J., Coventry, L., Jansen, J., & Kusev, P. (2017). Risk perceptions of cyber-security and precautionary behaviour. C*omputers in Human Behavior*, *75*(75), 547–559. https://doi.org/10.1016/j.chb.2017.05.038

Vishwanath, A., Harrison, B., & Ng, Y. J. (2016). Suspicion, cognition, and automaticity model of phishing susceptibility. C*ommunication Research*, *45*(8), 1146–1166. https://doi.org/10.1177/0093650215627483

Vishwanath, A., Neo, L. S., Goh, P., Lee, S., Khader, M., Ong, G., & Chin, J. (2020). Cyber hygiene: The concept, its measure, and its initial tests. *Decision Support Systems*,

128, 113160. https://doi.org/10.1016/j.dss.2019.113160

von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. C*omputers & Security*, *38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

Wang, J., Liu-Lastres, B., Ritchie, B. W., & Mills, D. J. (2019). Travellers' self-protections against health risks: An application of the full Protection Motivation Theory. *Annals of Tourism Research*, *78*, 102743. https://doi.org/10.1016/j.annals.2019.102743

Wang, Z., Zhu, H., & Sun, L. (2021). Social Engineering in cybersecurity: Effect mechanisms, human vulnerabilities and attack methods. *IEEE Access*, *9*, 11895–11910. https://doi.org/10.1109/access.2021.3051633

Warkentin, M., McBride, M., Carter, L., & Johnston, A. (2012). The role of individual characteristics on insider abuse intentions. *AMCIS 2012 Proceedings*, *28*.

Warkentin, M., Walden, E., Johnston, A. C., & Straub, D. W. (2016). Neural correlates of protection motivation for secure IT behaviors: An fMRI examination. *Journal of the Association for Information Systems*, *17*(3). https://doi.org/DOI: 10.17705/1jais.00424

Wiafe, I., Koranteng, F. N., Obeng, E. N., Assyne, N., Wiafe, A., & Gulliver, S. R. (2020). artificial intelligence for cybersecurity: A systematic mapping of literature. *IEEE Access*, *8*, 146598–146612. https://doi.org/10.1109/access.2020.3013145

Witsenboer, J. W. A., Sijtsma, K., & Scheele, F. (2022). Measuring cyber secure behavior of elementary and high school students in the Netherlands. C*omputers & Education*, *186*, 104536. https://doi.org/10.1016/j.compedu.2022.104536

Workman, M. (2007). Gaining access with social engineering: An empirical study of the threat. *Information Systems Security*, *16*(6), 315–331. https://doi.org/10.1080/10658980701788165

Zeadally, S., Adi, E., Baig, Z., & Khan, I. (2020). Harnessing artificial intelligence capabilities to improve cybersecurity. *IEEE Access*, *8*, 1–1. https://doi.org/10.1109/access.2020.2968045

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

APPENDIX 1: INTERVIEW GUIDE

Consent Letter signed by participants

Proforma Consent Letter

Dear Participant,

I am a student at the University of Pretoria's Gordon Institute of Business Science and completing my research in partial fulfilment of an MBA. I am conducting research on cybersecurity and trying to discover more about factors affecting people's attitude towards cybersecurity in the workplace. Our interview is expected to last about an hour and will help us understand how cybersecurity professionals and organisational leaders can shape their cybersecurity programmes in their efforts to fight against the ever-increasing cyber-risk phased by organisations and individuals.

Your participation is voluntary, and you can withdraw at any time without penalty. All data will be reported without identifiers. If you have any concerns, please contact my supervisor or me. Our details are below.

Researcher name: Naomi Mahlatje	**Research Supervisor Signature**
Email: naomi.mahlatje@gmail.com	**Email**: Suzanne.myburgh@hotmail.com
Phone: 072 704 0396	**Phone**: 072 406 9191

Signature of participant: _____

Date: _____

Biographical questions:

- Tell me about your current role.

    Planned prompt: How does your typical day or week look like?

    Planned prompt: How long have you been in this role?

    Planned prompt: Which division / department do you work in?

    Planned prompt: What is your title?

Main interview questions:

Propositions	**Interview Question**
Proposition 1: Cybersecurity awareness and training shapes employees on the organisational and individual cyber-risk perceptions	1. How would you define of cyber-risks encountering individuals and organisations today?
	2. In your view, are South African organisations doing enough to protect their businesses from cyber and data breaches?

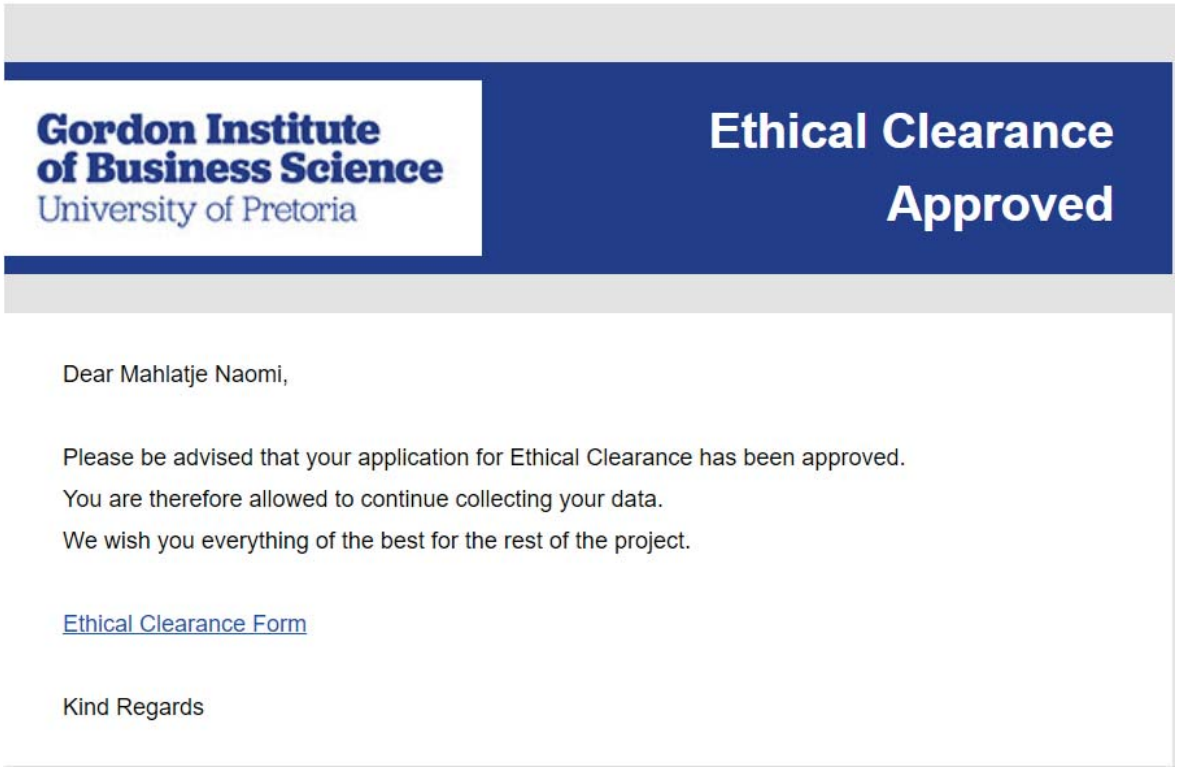
Propositions	Interview Question
	• *Planned prompt* - Why do you think that is the case? • *Planned prompt (If participant's view is that organisations are not doing enough)* – what more do think needs to be done?
	3. What is your view on regulations aimed to protect people's privacy, such as POPIA and GDPR?
	4. When talking about cyber-risk, what example of an adverse cyber breach comes to your mind? • *Planned prompt:* What do think the organisation in question should have done better to prevent the incident?
Proposition 2: Individual cyber-risk perception functions as a lever for protective cyber behaviour in the workplace	5. What is your view on the effectiveness of the cybersecurity awareness training programmes? *Planned prompt:* Do you think these should be mandatory or participation choice be left to employees? Why?

Propositions	Interview Question
	6. Do you think that you are inclined to be targeted for a cyberattack? Why? • *Planned prompt:* If you were to be targeted for a cyberattack, how severe do you think the consequence of such attack would likely be? • *Planned prompt,* how do you protect yourself against cybercrime as an individual? • *Planned prompt:* How do you or would you handle a cyberattack if you were targeted?
	7. Would it concern you if you knew that the laptop that you are working on does not have an anti-virus enabled? Why? • *Planned prompt* – would you install it yourself install yourself of would you seek help?
Proposition 3 **Organisational cyber-risk perception**	8. In your view, should organisations allow their employees to use their personal devices to access company data and systems? • *Possible prompt (if Yes)* – how do you think that this would influence the

Propositions	Interview Question
does not directly shape individual protective cyber behaviour	organisation's cyber-risk? • *Possible prompt (If No)* – how do you think this would influence employee productivity? • *Possible prompt*: How can organisation get a balance between security and productivity in this regard? • *Possible prompt:* In the organisation that you work for, how are personal devices treated? Do you think this is a fair approach?
	9. When working on company devices, do you think that organisations should block certain things, such as USB ports, use of public emails, such as Gmail or cloud storages, such as G-Drive? • *Possible prompt (If Yes)* – what consequences do you think this can have on employee's attitude to cybersecurity or the organisation in general? • *Possible follow up question (If No)* - how do you think that this would influence the organisation's cyber-risk? • *Possible prompt* How can organisation get a balance between security and productivity in this regard?

Propositions	Interview Question
	• *Possible prompt:* In the organisation that you work for, how are personal devices treated? • *Possible prompt:* In the organisation that you work for, how USB's, public emails and public cloud providers treated? Do you think this is a fair approach?

APPENDIX 2: ETHICAL CLEARANCE



Gordon Institute of Business Science
University of Pretoria

Ethical Clearance Approved

Dear Mahlatje Naomi,

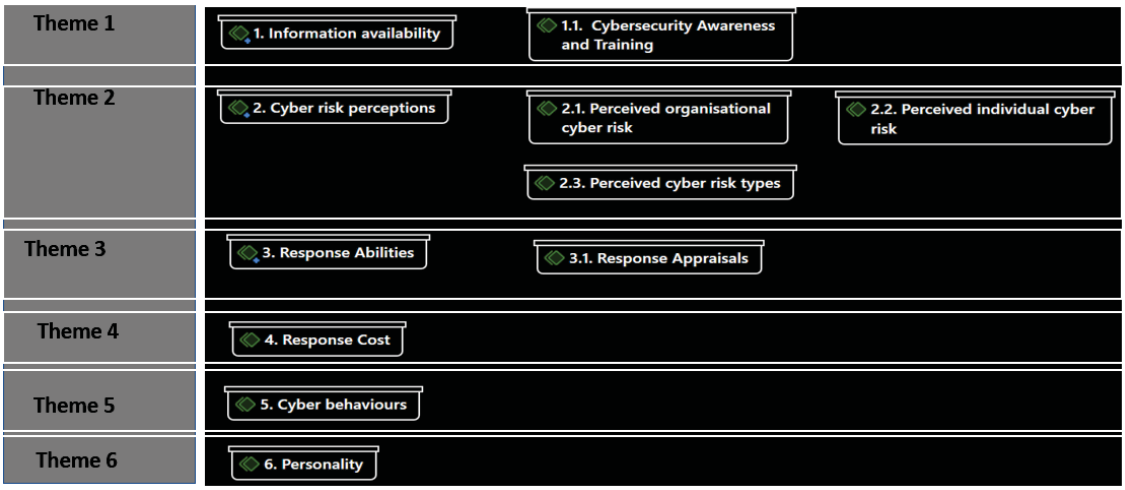
Please be advised that your application for Ethical Clearance has been approved.
You are therefore allowed to continue collecting your data.
We wish you everything of the best for the rest of the project.

Ethical Clearance Form

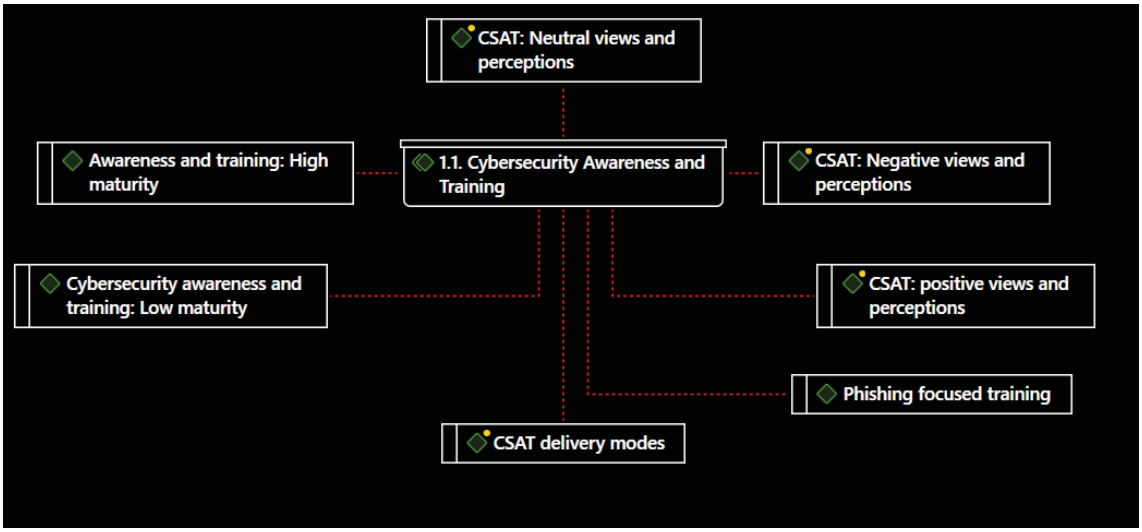
Kind Regards

APPENDIX 3: CODEBOOK

Level 0 codebook showing main themes and categories

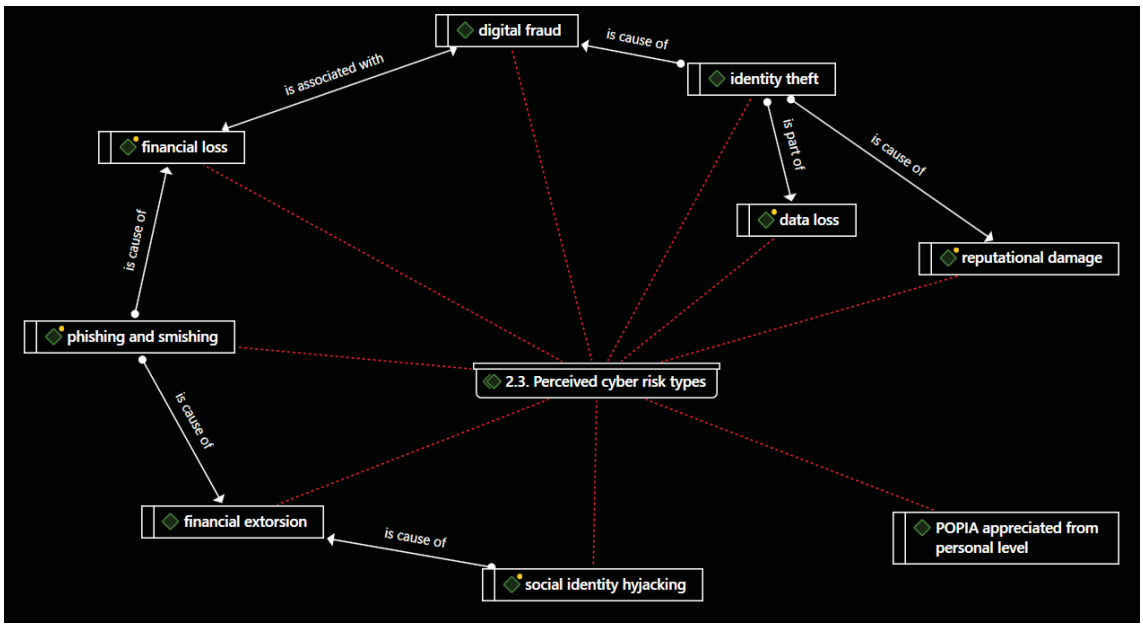


Theme 1: Cybersecurity Awareness and Training

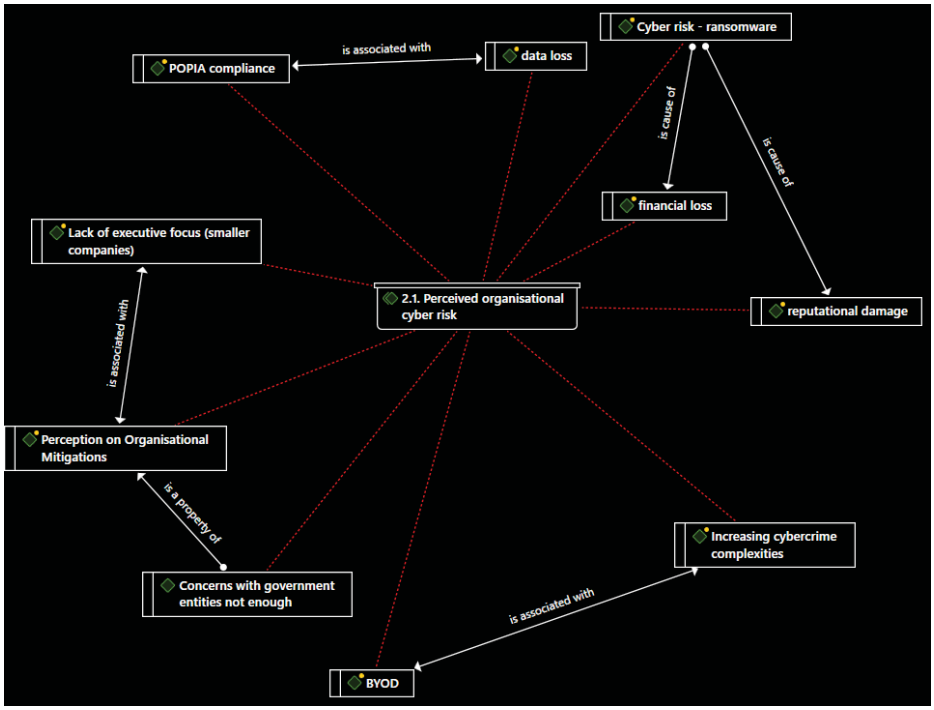


Theme 2: Cyber-risk perceptions

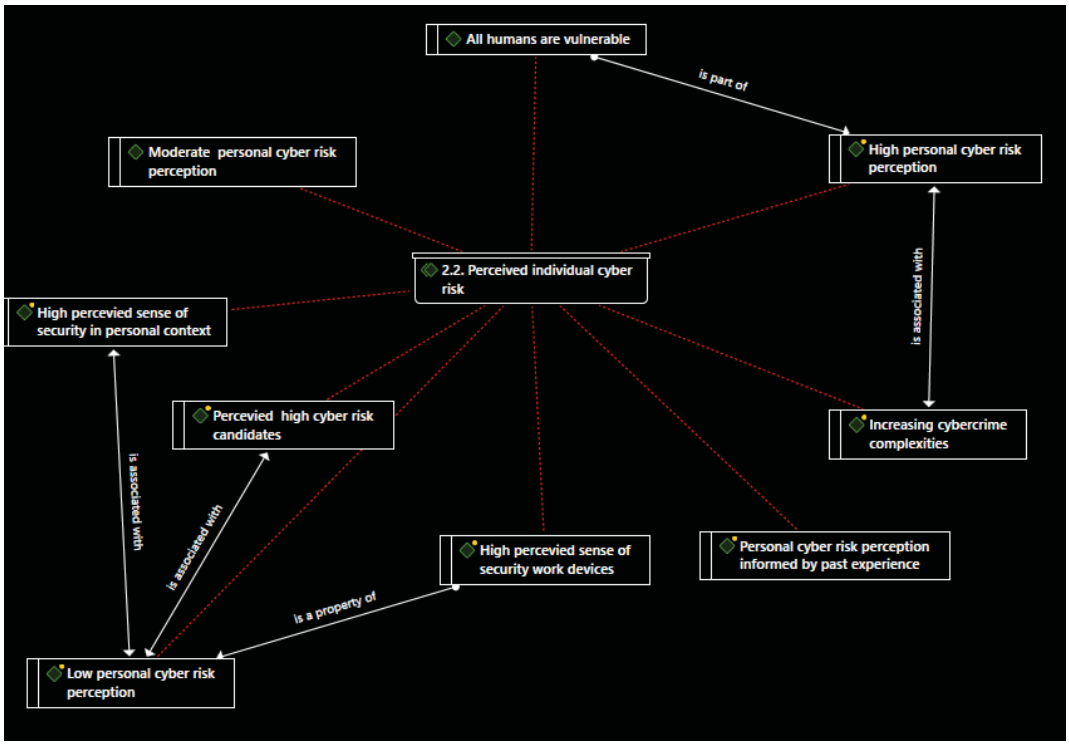
Perceived individual cyber-risks



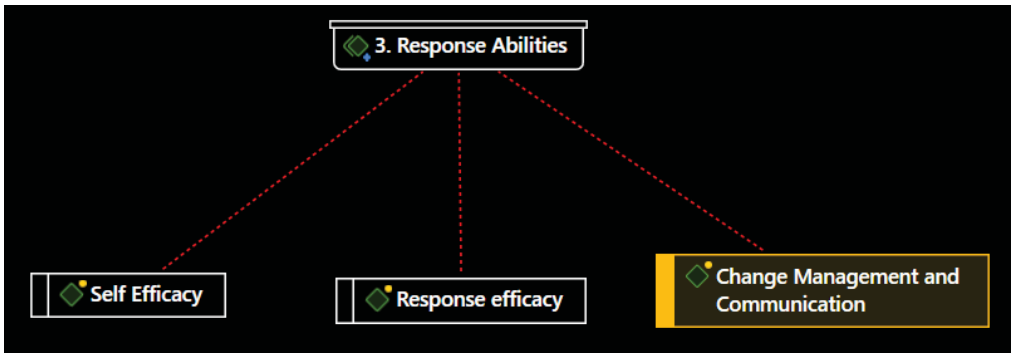
Perceived organisational cyber-risks



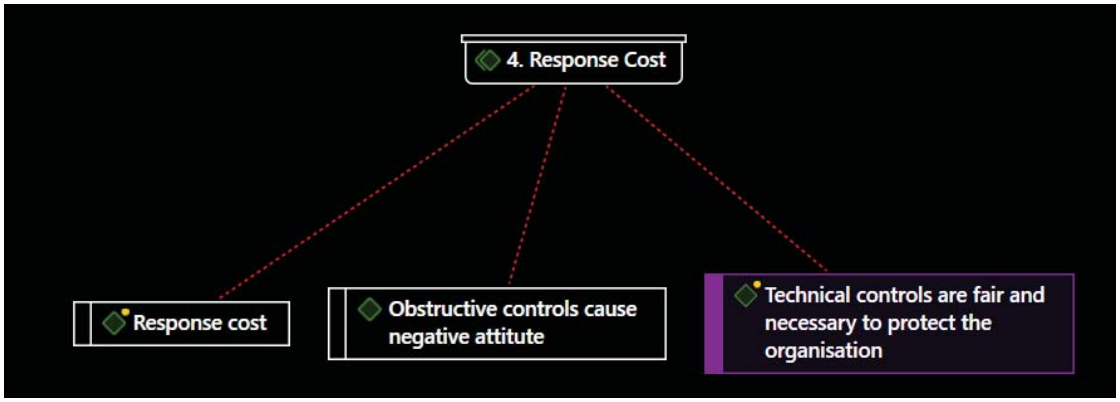
Perceived individual cyber-risks



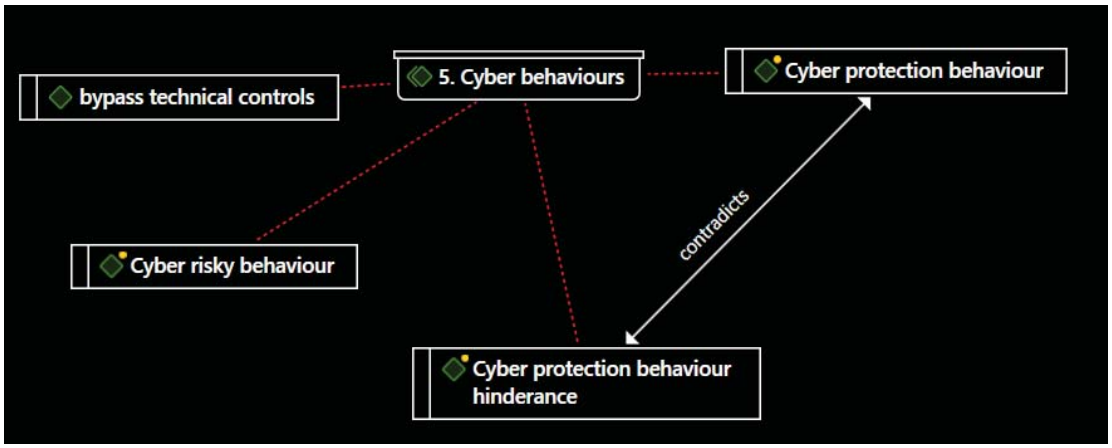
Theme 3: Cyber response abilities



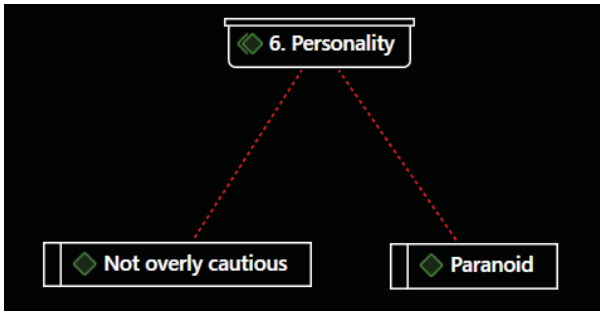
Theme 4: Response Cost



Theme 5 Cyber behaviours



Theme 6 Personalities



APPENDIX 4: EDITING CERTIFICATE

Nr: 202673

ACADEMIC AND PROFESSIONAL EDITING SERVICES

Tel nr: USA: +1 (773) 217-4568/ NZ: +64 22 359 2202 SA +27 81 534 3590/
www.apespro.com; Facebook: www.facebook.com/apespro

LANGUAGE EDITING CERTIFICATE

Report title:	The role of cybersecurity awareness and training in shaping cyber risk perceptions and resultant cyber behaviours
Author/s:	Naomi Mahlatje
Institution:	Gordon Institute of Business Science
Date Issued:	30 October 2022

This document certifies that the manuscript listed above was edited for proper English language, grammar, punctuation, spelling, and overall style. Neither the research content nor the author's intentions were altered in any way during the editing process. Documents receiving this certification should be English ready for publication; however, the author has the ability and choice to accept or reject our suggestions and changes.

APES does not take responsibility for plagiarism.

If you have any questions or concerns about this document or certification, kindly contact: Info@apespro.com

APES is committed to providing high-quality services for professionals and researchers. To find out more about APES, visit www.apespro.com.

Warm regards

Elizabeth Marx

Attended the EFA International Editors' Conference – Chicago: August 2019 https://www.the-efa.org/efas-2019-conference-announcement/