Digital Risk Management: Investigating Human-Factor Security with a Behaviourist Approach

by

Ruan Pretorius

Thesis presented in fulfilment of the requirements for the degree of
Master of Arts in the Faculty of
Socio-Informatics at Stellenbosch University

Supervisor: Mr. DN Blaauw
Co-supervisor: Prof. BW Watson

April 2022

Centre for AI Research School for Data-Science & Computational Thinking

Declaration

By submitting this thesis electronically, I declare that the entirety of the work contained therein is my own, original work, that I am the sole author thereof (save to the extent explicitly otherwise stated), that reproduction and publication thereof by Stellenbosch University will not infringe any third-party rights and that I have not previously in its entirety or in part submitted it for obtaining any qualification.

April 2022

Abstract

Digital Risk Management: Investigating Human-Factor Security with a Behaviourist Approach

Ruan Pretorius

Department of Information Science
University of Stellenbosch

Thesis: MA (Socio-Informatics)

April 2022

The successful digitisation of modern organisations relies on the cohesion between information technology and the workforce responsible for managing and operating it. Without proper management and operation, even the most sophisticated technologies may become vulnerable when operated by a low skilled worker. Numerous studies acknowledge human vulnerability in cyber security, also known as human-factor security, as the "weakest link" in a digitised organisation's security posture. Existing literature suggests that there is a lack of focus on the impact of human-factor security on information and data security in organisations. The focus is on the risks posed by technologies, whereas the risks presented by workers implementing, managing, or interacting with these technologies are neglected. In addition, existing literature proposes risk management frameworks to aid in digital risk management as a whole. Thus, the need to investigate how risk management frameworks could be applied to human-factor security in digitised organisations arise. This paper provides a comprehensive understanding of the behavioural and cognitive science of people in relation to digital threat awareness and response. This is achieved through a qualitative assessment of responses to survey questions on an authentic dataset. This authentic dataset consists of South African employees working in digitised orginisations. The survey questions utilise the Behaviourist Learning Theory. The Behaviourist Learning Theory relies on understanding human behaviour by investigating the person's behvioural response when exposed to environmental stimuli. For this survey, the

behaviour is understood by investigating the partcipants' behvioural response when exposed to digital threats. The survey results give an indication of the strength of the security posture of the dataset. Additionally, from the survey results, insight is gained on how the human-factor security may be improved. Therefore, a risk management plan is presented to assist in managing human-factor security. The risks management plan involves the identification, assessment, response to the risks found in the behaviour from the dataset. Thus, this research project provides security- and risk managers with insight into human vulnerabilities and behaviour when interacting with information systems and technology in digitised organisations. The insights presented in this paper may be utilised to enhance the organisation's security posture through the implementation of a risk management plan. From the survey responses, it is evident that most respondents show a high level of awareness of security and competence when exposed to potential threats. However, there can be observed that few employees do portray risky behaviour. The risky behviour may still result in devastating consequences, regardless of the low probability of occurrence.

Uittreksel

Digitale Risikobestuur: 'n Gedragskunde Benadering tot die Ondersoek van Menslike Faktor Sekuriteit

Ruan Pretorius

Thesis: MA (Socio-Informatics)

April 2022

Die suksesvolle digitalisering van moderne maakstappye steun op die kohesie tussen informasie tegnologie en die werksmag verantwoordelik vir die bestuur en bedryf daarvan. Sonder behoorlike bestuur en bedrywing kan selfs die mees gesofistikeerde tegnologieë kwesbaar wees in die hande van 'n onbekwame werker. Talle studies toon dat menslike kwesbaarheid in kuber-sekuriteit die “swakste-skakel” in 'n digitale maatskappy is. Menslike kwesbaarheid in kuber-sekuriteit is ook bekend as menslike-faktor sekuriteit. Die literatuur stel voor dat daar 'n tekort ontstaan van die fokus op die impak wat menslike-faktor sekuriteit op inligting and data sekuriteit in organisasies het. Die fokus word meestal geplaas op die risiko wat tegnologie bring en daardeur skep dit die risiko wat die werksmag bring af, wat hoofsaaklik hierdie tegnologieë bestuur en bedryf. Verder stel bestaande literatuur risiko bestuurs raamwerke voor met die doel om risiko bestuur as 'n geheel te verbeter. Daardeur onstaan die behoefte na die ondersoek oor hoe risiko bestuurs raamwerke toegepas kan word in menslike-faktor sekuriteteit in maatskappye. Hierdie projek bied 'n omvattende begrip van die gedrags en kognitiewe wetenskap in verband met die bewustheid en reaksie op digitale bedreigings. Verder is daar 'n risiko-bestuurs plan opgestel wat ondersteuning bied vir die bestuur van menslike-faktor sekuriteit. Dit word bereik deur 'n kwalitatiewe assessering van antwoorde op opnamevrae op 'n unieke datastel. Hierdie unieke datastel bestaan uit Suid-Afrikaanse werknemers wat in gedigitaliseerde organisasies werk. Die opnamevrae gebruik die *Behaviorist Learning Theory*. Die *Behaviorist Learning Theory* maak staat op die verstaan van menslike gedrag deur die persoon se gedragsreaksie te ondersoek wanneer dit aan omgewingstimuli blootgestel word. Die antwoorde op die opnamevrae gee ’n indikasie van die sekuriteitspostuur van die datastel. Die opname resultate bied insig oor hoe die menslike faktor

sekuriteit verbeter kan word. Daarom word 'n risikobestuursplan aangebied om te help met die bestuur van menslike faktorsekuriteit. Die risikobestuursplan behels die identifikasie, assessering, reaksie op die risiko's wat in die gedrag van die datastel gevind word. Hierdie navorsings projek voorsien sekuriteits bestuurders met waardevolle insig. Hierdie insig ondersteun die begrip van die gedrag en kwesbaarheid wat die werksmag toon teenoor die bedrywing van tegnologieë en inligtingstels in maatskappye. Hierdie insig kan aangewend word om 'n organisasie se sekure postuur te verbeter deur 'n risiko bestuursplan aan te wend. Deur die opname is dit duidelik dat die meerderheid van die werskmag reeds 'n hoë vlak van risiko bewustheid en reaksie toon in die moontlike blootstelling aan bedreidings. Alhoewel, daar kan gesien word dat sommige werkers wel hoë-risiko gedrag toon, wat ‘n bedreiging vir ’n maatskappy se digitale sekuriteit kan wees. Hierdie hoë-risiko kan na groot skade vir 'n maatskappy lei, ongeag van die lae waarskynlikheid dat dit sal plaasvind.

Acknowledgements

I would like to express my sincere gratitude towards the following people: I would like to acknowledge my supervisors, Mr. Dewald Blaauw & Prof. Bruce Watson for the support and guidance they provided me within our regular discussions. I thank them for their sincerity when discussing and listening to my ideas and nudging me in the right direction. Additionally, I would like to thank my friends and family for their support and for motivating me in difficult times and throughout the lifespan of this project.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Background

Cyber threats aim to exploit the shortcomings within digitised companies. In many cases, the workers can be regarded as one of the weakest links in terms of cybersecurity. While the advancement of technology allows for more complex and sophisticated systems, various challenges and cyberthreats are introduced simultaneously. Thus, the more complex technology becomes, the more people are susceptible to making unintentional mistakes or errors that put the organisation at risk. It is far easier to exploit humans than it is to exploit secure information systems or technology. Cyberthreats are magnified when managers of digitised companies overestimate the security of technology, while also neglecting the effects of human error. It is clear that the impact and management of humans are a crucial element in cyber security.

Employees can pose as one of the greatest internal risks to digitised companies. Therefore, the success of digitised organisations and the efficacy of information systems rely greatly on the employees who manage and interact with technological systems. As a result, the human role in digital risk management is of cardinal importance for organisations to establish a strong security posture.

The human role in digital risk management is referred to as human-factor security. Furthermore, within the information security environment, human vulnerability refers to any human weakness that could potentially be exploited by an attacker that leads to the compromise of valuable or sensitive information (Tungal, 2021). Therefore, human vulnerability may be described as any human behaviour that may render information systems susceptible to unintentional or malevolent harm. Therefore, human vulnerabilities must be managed successfully in order to strengthen human-factor security.

This research project aims provide insight into human-factor security and human behaviour when interacting with information systems. These insights shall be used to provide suggestions to improve risk management. A literature review on human vulnerabilities in cybersecurity, as well as various existing risk management models, will be presented.

Insight into human-factor security shall be provided through the qualitative assessment of responses to survey questions on an authentic dataset. This authentic dataset consists of South African employees working in digitised orginisations. The survey questions shall utilise the Behaviourist Learning Theory. The Behaviourist Learning Theory relies on understanding human behaviour by investigating the person's behvioural response when exposed to environmental stimuli. Through this survey, the behaviour is understood by investigating the partcipants' behvioural response when exposed to digital threats. The survey results shall give an indication of the strength of the security posture of the dataset. Furthermore, the insights from the survey results shall aid in developing suggestions for improving human-factor security, as well as formulating a risk management plan to assist in managing human-factor security. The risks management plan involves the identification, assessment, response to the risks found in the behaviour from the dataset.

1.2 Problem Statement

The impact and risk that human workers hold in terms of information and data security for an organisation is greatly underestimated (Evans et al., n.d.; Nobles, 2018). Currently, a greater focus is placed on the risks posed by technologies, when compared to the risks posed by the workers implementing, managing, or interacting with these technologies. Even the most sophisticated technology can become vulnerable when operated by a low skilled worker. The existing literature focusses on the general principles of risk management strategies. None of the existing papers focus extensively on the application of risk management on human-factor security within digitised companies. Additionally, the existing risk management strategies are rarely tested with an authentic dataset. Furthermore, none of the existing studies implement Behaviourist Learning Theory to understand the behaviour of people when exposed to the stimuli of digital threats. These threats are present in the day-to-day activities of all people in the workplace (onsite) and offsite.

An in-depth understanding of the behavioural and cognitive science of people in relation to digital threat awareness and response is needed. Thereby, insight can be gained on how to decrease their vulnerability and susceptibility to cyber threats. A comprehensive research and analysis of organisational as well as digital risk management strategies are needed in order to understand its level of success and effectiveness.

1.3 Research Questions

The purpose of this study is to gain a comprehensive understanding of human-factor security within information security, with the goal to improve risk management in digitised organisations. Therefore, the following questions arise:

1. Are current risk management strategies used in companies effective at managing security risks and threats? (RQ1)
2. What are the strengths and shortcomings found among digital risk management strategies/frameworks within literature? (RQ2)
3. Are modern digitised organisations aware of the impact and vulnerability of the workforce related to cyber threats? (RQ3)
4. Do digitised companies implement risk management strategies that cater for or mitigate potential threats caused by the workforce? (RQ4)
5. Does the average worker possess the level of knowledge, skill, and risk awareness in order to implement adequate security measures in their day-to-day activities within organisations? (RQ5)
6. Is environmental stimuli-behaviour investigation effective enough at gaining an understanding of behaviour when potentially exposed to cyber/digital threats? (RQ6)

1.4 Research Design

Firstly, a comprehensive literature shall be presented, which focusses understanding human behaviour and human-factor security, as well as digital risk management strategies in digitized orginisations. The knowledge and background acquired from the literature review conducted will serve as the foundation from which the empirical will be executed. The literature review shall provide an understanding of how and why humans react to certain digital threats. In

addition, the human behaviour that cause risks for organization shall be identified. This understanding will aid in the formulation of questions for the survey.

Secondly, empirical data shall be collected. Data will be collected in the form of electronic surveys that will be delivered to participants via word of mouth and social media invitation. The survey shall consist of various sections, which shall be described in detail in Chapter 3. In one of the survey sections, the Behavioral Learning Theory shall be utilised to investigate different stimuli-response scenarios, wherein the respondent's behavioural responses to various digital threats are examined.

Thirdly, a qualitative analysis on the survey responses shall be done to try to determine the strength of the security posture of the data set, as well as evaluate trends in the data set.

Finally, a risk management plan shall be developed from the insights gained from the survey responses. The risk management plan includes the identification and assessment of the risks found the behaviours exhibited by the respondents from the survey. Thereafter, measures to eliminate or mitigate the potential risks are proposed.

1.5 Outline of the Thesis

Within this chapter, a succinct overview of the background, problem statement, research questions and research design were provided for the underlying research project. The remainder of chapters are presented as follows:

Chapter 2 provides an in-depth review of relevant literature and consists of two sections. The first section of the literature review focuses on human vulnerability in digitised organisations. The focus is on the understanding of human behaviour in cyber threats, what influences behaviour, what causes people to make errors that leads to risks, how people perceive risks, how people react when exposed to risks and lastly, threats and the vulnerabilities attackers seek to exploit. The second section of the literature review focuses on risk management and strategies in organisations in general as well as specifically digitised organisations. Digitised organisations incorporate technology in various facets of the orginisation with the aim to increase efficiency, enhance their customer experience, and increase sales. These strategies include risk identification, assessment, and mitigation of various types of cyber threats an

organisation can be faced with, also known as “digital risks”. Additionally, there will be focused on the key aspects of risk management and more specifically, the role and impact that the human employee has on risk management.

Chapter 3 presents the methodology and design of research. This project utilises a survey methodology for data collection, thus placing emphasis on structure and design of the questionnaire. Additionally, this section describes the goal and motivation of the survey as well as the execution process and management.

Chapter 4 presents mainly a qualitative analysis conducted on the data collection obtained from the survey, with the addition of quantitative grouping of the results. Additionally, this section includes a risk assessment conducted in the survey results which is described in detail, as well a summarised table of the assessment findings and results.

Chapter 5 presents a discussion and interpretation of the results for each individual section of the survey as well as the discussion on the answering of the research questions.

Chapter 6 presents a conclusion of the study, which is aided by an overview of the limitations of the study and recommendations for future research.

Chapter 2

Literature Review

2.1 Human vulnerability within the digitised organisation

Human related errors were reported to be the second largest cause for security breaches in organisations (Kaspersky, 2020). In addition, over 52% of businesses in 2020 admitted that their employees are the leading contributor to digital security risks. Human related errors can occur in many ways and can introduce a wide variety of threats for organisations that put their valuable assets and information at risk. These human related errors can be referred to as human-factor security (Ani et al., 2019). By neglecting or misjudging human-factor security, organisations are prevented from capitalising on technological advances, as these technologies are still implemented and managed by humans (Nobles, 2018). Technology is potentially just as weak as the workers who develop and operate it (Ani et al., 2019).

The following section presents an investigation of human vulnerability within digitised organisations in relation to data and information security. More specifically, the investigation is based upon three main subjects; how risk perception and personal biases influence actions, the specific human vulnerabilities and errors that attackers/hackers seek to exploit. Lastly, how insight to human behaviour by focusing on the various internal (personal) and external (information system interaction, organisational culture) factors that influence behaviour and potentially cause risks.

2.1.1 Risk perception

Human behaviour in information security is influenced by many factors that are related to individuals personally, such as risk perception. Many studies consider risk perception as a crucial element in the understanding of human reactions when faced with certain threats (Bada & Nurse, n.d.).

Bada & Nurse (n.d.) highlights that people are more concerned by the effects or outcome of an attack rather than the attack itself. Furthermore, the steps taken to address threats vary amongst

individuals (Bada & Nurse, n.d.). Thus, understanding how people perceive risks are crucial in determining their behaviour and actions. Through studies it is found that risk perception is influenced by individuals' personal heuristics, as well as their information processing biases (Parsons et al., 2010). It is also suggested that an individual's interpretation of facts through personal beliefs, values, attitudes and judgement may also influence risk perception (Bada & Nurse, n.d.). Thereby, individuals' actions are determined by the accuracy of their perception accompanied by their interpretation of facts of risks associated with their actions. Bada & Nurse (n.d.) expand on an individual's beliefs by stating that an individual's motivation and action towards a security risk depends on their personal beliefs of the impact of threats. This includes the severity of an event of threat, their susceptibility to the threat and their perceived ability to apply preventative or mitigation actions towards the threat. The various heuristics and biases analysed by Parsons et al., (2010) is based upon individuals' estimation of risks, optimism, personal level of control, knowledge, risk homeostasis, omission biases, familiarity influence, risk framing, personality, and cognition and lastly, social impact.

The estimation of risks is influenced by media coverage regarding the risks, meaning that risks that are common and chronic are reported less and underestimated, whereas risks that are rare and more severe are overestimated. Through optimism bias people tend to believe that hackers would perceive their information as less valuable, thus portraying a false sense of immunity against attacks (Parsons et al., 2010). People tend to disregard the absence of warning signs of attacks as being exempt from attacks, when in fact, attackers can choose any person as victim to gain access to the larger system. An individual's level of control over actions also determines their level of optimism and thereby underestimates the riskiness of threats. People who portray a stronger sense of control tend to indulge in riskier activity because of their perceived ability to manage the occurrence of threats. Through risk homeostasis the amount of risk taken by individuals is conditional based on the level of risk associated with an action. Thus, when people perceive a condition as riskier, the chance that they will indulge in the activity and vice versa when they perceive a condition as less risky. The omission bias occurs when an individual regards an omission act as more acceptable than that of a commission. Here, an omission act refers to the act of forgetting to perform crucial actions, while a commission act refers to performing incorrect action. As a result, this leads to the occurrence of *post-completion errors*. *Post-completion errors* can also be as a result of *capture errors*, where habitual behaviour takes over unfamiliar activities (Parsons et al., 2010). This error occurs when an individual habitually clicks "OK" in every situation without proper consideration of the potential risk associated

with this action. These errors usually occur when an individual suffers from tiredness or lack of concentration. The familiarity of risks affects behaviour. The more familiar a risk or the occurrence of a risk, the more the risk is underestimated and the higher the chance of an individual indulging in a risky action. Risk framing refers to the manner a risk is described or portrayed. More specifically, when a risk is described with emphasis on the potential losses, the outcome results in more risk-taking actions. When a risk is described by the potential gains, the result is more risk-averse actions. Risk taking behaviours are also influenced by personality and cognition. People who seek out risks tend to focus on the rewards associated with the risks and people who are risk-averse tend to focus on the losses associated with the risks and are less likely to indulge in risky activities. Bada & Nurse (n.d.) states that the culture of fear regarding a threat and the dangers associated with it can also be a driver of behaviour. Social factors such as groups and norms also affect individuals' behaviour (Bada & Nurse, n.d.). Individuals tend to dictate the beliefs and perceptions of risks and norms that are portrayed within groups. Lastly, people continuously indulging in activities that are perceived as low risk at a given time could cumulatively build up to potentially become a serious or high risk in the future.

Bada & Nurse (n.d.) expands on the concept of risk perception by stating that the level of perceived exposure to certain risks influences how risk is perceived through the public eye. The various levels of risk exposure are perceived by individuals as either voluntary or involuntary, by the level of familiarity of the risk in society or by the level of perceived controllability over the risk. Furthermore, this includes whether the risk is targeted or at random and the level of fear aroused by the risk. Others delve deeper into human behaviour and psychological predispositions in order to explain and prevent social engineering attacks and susceptibility (Briggs et al., n.d.; Conteh & Schmick, 2016)

2.1.2 Vulnerability, errors, and exploitation

Within the information security environment, human vulnerability refers to any weakness that could potentially be exploited by an attacker that leads to the compromise of valuable or sensitive information (Tungal, 2021). The errors that humans inevitably make when using IT systems can expose vulnerabilities in the IT systems. These vulnerabilities can be exploited to attack the system. This section will discuss human vulnerabilities, how these vulnerabilities are caused and how it is targeted and exploited by attackers.

According to an investigation done on global case studies for the Verizon's 2020 Data Breach Investigations Report, the six biggest ways through which data breaches occur are criminal hacking, human errors, social engineering, malware, unauthorised use and lastly, physical actions (Irwin, 2020). Human errors and social engineering alone account for 44% of the causes of data breaches. With a closer look at the other data breach causes highlighted by Irwin (2020), it is clearly visible that the human employee plays a potential part in every cause. With criminal hacking, the attacker can use credentials obtained in a nefarious way from employees to gain access and infiltrate the organisation. With malware, attackers can infect vulnerable or unskilled employees' computers to gain access and infiltrate an organisation. Through unauthorised use, an employee can mishandle valuable information, abuse their privileges, or simply not follow access policies and procedures. These actions can be with or without malicious intent. Stanton et al., (2005) expands on behavioural intent by providing a two-factor taxonomy that classifies end-user security behaviour. As seen in figure 1, six behaviour categories could be derived from the two-factor matrix.

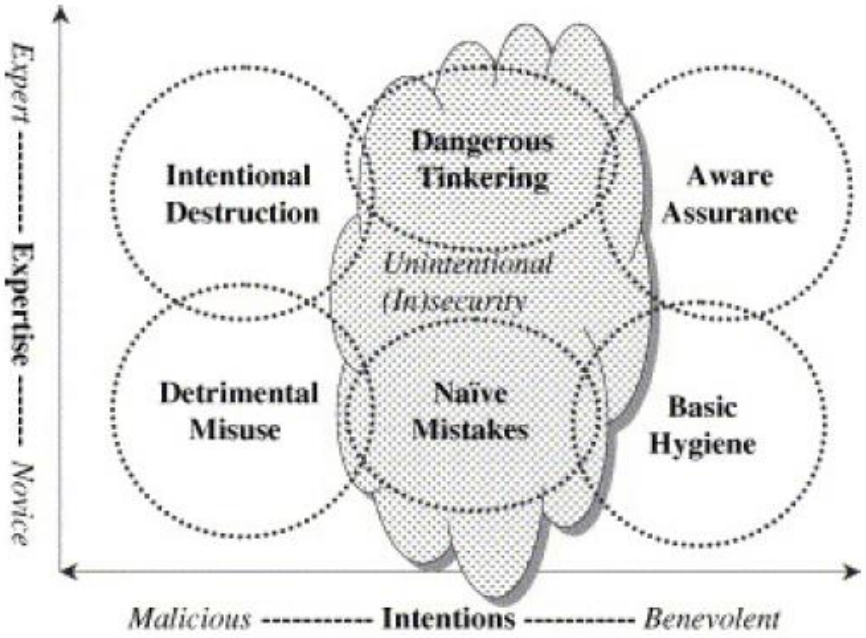

Figure 2.1: Two-factor taxonomy of end user security behaviours (Stanton et al., 2005)

With regards to intent, the matrix identifies two categories for intentional behaviour and two for unintentional behaviour. "Intentional destruction" refers to people who have the technical expertise and malicious motives. Whereas with "Detrimental Misuse", people have malicious

intentions or motives but lack technical expertise. With regards to unintentional behaviour, “Dangerous Tinkering” refers to people who have the technical expertise to do damage but have no malicious intent. “Naive Mistakes” are seen as the most common type of behaviour where people with low technical expertise and no malicious intentions to do harm perform any action that could cause a security breach. From a recent study conducted by IBM regarding cyber breaches it was found that human error is the largest contributor in 95% of breaches (The Hacker News, 2021).

Through physical actions such as theft or loss of documents, sensitive information is vulnerable and at risk. Theft and loss of information can occur as a result of employees not following adequate safety controls and measures. All these various factors can potentially cause back doors to orgnisational information and data for criminals and attackers. To extend human errors as one of the main causes of information security breaches, Parsons et al., (2010) highlights four types of human-factor errors in order to explain these causes. Firstly, the act of omission which refers to people forgetting to perform crucial actions, secondly, the act of commission where the incorrect actions are performed, thirdly, actions that are unnecessary or irrelevant. Lastly, actions that are done out of sequential order or untimely.

When referring to exploitable vulnerabilities within individuals, according to Nurse, (2019) the main psychological traits that criminals sought to exploit are the willingness to trust, the impact that stress and anxiety has on decision making, personal needs and naivety in decision making. Attackers or criminals commonly use fear, trickery or deception as their weapon to exploit these psychological traits through personal persuasion or creating a contrived situation (Parsons et al., 2010). According to Nurse, (2019), phishing and spear-phishing are the most common strategies used by attackers to trick, deceive or socially engineer people in order to transmit malware. Phishing refers to the fraudulent act where an attacker sends messages, such as emails, and falsely claim to be from a reputable company to persuade huma victims to reveal personal information, such as passwords and credit card numbers, to the attacker, or to deploy malicious software on the victim's infrastructure, such as ransomware. Spear phishing targets a specific group of people or a specific type of individual, whereby the attacker tailors an email to speak directly to the victim and contains information only an acquaintance of the victim would know. This information is typically obtained after the attacker gains access to the victim’s personal data. Parsons et al., (2010) explains that human susceptibility is increased through situations where attackers trigger certain psychological responses within the victim.

Situations that may trigger psychological responses include: when an attacker is able to establish a level of trust with the victim; when a victim responds to an innocuous request for information not knowing that the information they provide can lead to a chain of other attacks; when attackers heighten the emotional state within the victim in order to distract and hinder the victims logical evaluation capabilities such as, excitement, fear, anger, guilt and empathy; when an attackers influence a victims level of commitment by creating a bond with the victim or using the "reverse social engineer" technique in order to obtain reciprocation from the victim. Through reverse social engineering the attacker creates a hypothetical problem whereafter the attacker generously offers to assist with the problem. This generous act by the attacker is thus executed with the aim to trigger appreciation and gratitude from the victim to retrieve their reciprocal assistance for more minor requests.

When referring to vulnerabilities within organisations directly related to the workforce, the main factors that causes vulnerabilities are the following: the complexity of information systems and technology; the connectivity of devices and technology; weak password management; the internet usage among the workforce, bugs in software that are knowingly or unknowingly placed by developers (Tungal, 2021). All these various factors rely on a single factor behind all vulnerabilities: the human worker.

Both Nurse, (2019) and Maalem Lahcen et al., (2020) emphasise the fact that stress and anxiety greatly affect decision making and cognitive ability, thus increasing the susceptibility to criminal attacks. It is clear that the lower the cognitive and decision-making ability, the higher the chances are for an error to occur and thereby and the higher a person's susceptibility to falling victim to an attack.

2.1.3 Behavioural insight

2.1.3.1 Personal influencers of behaviour

Many papers and reports emphasise the importance of behavioural insights to cybersecurity in order to understand what causes human susceptibility and vulnerability. Additionally, this includes how and why attackers exploit vulnerabilities and provide best practice theories to promote the improvement of behaviour. Briggs et al., (n.d.) investigated poor security behaviour by exploring different influencers of behaviour that are categorised as

environmental, *personal* and *social*. Through the study of these various influencers, it is clear that human behaviour is driven and influenced by a wide variety of factors. These factors are mainly the incentives and gratification of behaving in a certain way, personal factors such as knowledge, skill, attitude, perception and external influences such as peers, friends and family as well as the design and policies of information technologies. Maalem Lahcen et al., (2020)'s study provides extensive substance to the *personal* influencer identified in the report provided by Briggs et al., n.d.). Maalem Lahcen et al., (2020) describes 12 human factors that hinder performance and cognitive ability, leading to errors and incidents. These 12 factors include lack of communication, complacency, lack of knowledge, distraction, lack of teamwork, fatigue, which is also mentioned in the studies of Parsons et al., (2010) and Luciano, (2014), lack of resources, pressure, lack of assertiveness, stress, lack of awareness and norms. Luciano, (2014) states in their study that human behaviour in information security is mainly influenced by two aspects; an individual's personal characteristics, that is not related to cognitive ability such as values, beliefs and principles, and also, the organisational environment such as organisational culture, the colleagues and organisational values. (Parsons et al., 2010) describes two human errors that could occur as a result of tiredness and distraction or inattention: *capture errors* and *post-completion errors*. *Capture errors* occur when an individual performs an action where the familiar activity or routine overshadows an unfamiliar activity such a person deliberately clicking the "OK" button without considering potential consequences. Briggs et al., (n.d.) also identifies this habitual action as a reason why people are non-compliant with security best practices. *Post-completion errors* refer to actions where an individual neglects or forgets to carry out a final or "finish-up" action after a main goal has been completed. Examples of such actions are forgetting to shut down or log out of your computer after a day's work.

With the focus on personal traits and characteristics, it is thus clear that behaviour in information security is influenced by personal characteristics. More specifically these characteristics are directly related to mentality, cognition and affects cognitive ability, and characteristics that are related to personality and personal background such as biases, beliefs, values, and perceptions.

2.1.3.2 The complexity and interactions with information systems and technology

Many studies state that an information system is just as vulnerable as the people who operate it. Therefore, the interaction with these systems is one of the root causes of breaches. Whether

it is an employee with little technical ability, with malicious or non-malicious intent, or simply the information system being too complex the be efficiently operated, all the variables pose as potential risks that could eventually lead to breaches.

According to The Hacker News (2021), 95% of breaches are caused as a result of a human error. The majority of human errors with regards to the use of technology occur as either accidentally or unintentionally. According to Furnell (2005) accidental or unintentional errors mainly occur as a result of the problematic experience that people may encounter when interacting with information systems or technology. This includes the usability and understandability of the systems' security features. However, this problematic experience can occur either when an employee joins a new organisation, or when a new information system is required or being implemented, thus forcing change upon the workforce. Through a case study on technological change and adaption in organisations, Delaney & Delaney (2015) found that the usability is a crucial factor for the management and acceptance of a technology. Additionally, Delaney & Delaney (2015) states technological changes such as the implementation of an information system can bring many challenges, which all affects both organisation and the workforce. These challenges are among others change management, employee intimidation, uncertainty, discomfort, increased workload, required training, organisational culture and organsisation politics. It is thus in the hands of management to understand and address the needs and emotions of the employees by providing appropriate and adequate training and motivation. Thereby, a positive perception regarding the use of an information system or technology can be established. Delaney & Delaney (2015) suggests that if a technology is problematic or being newly implemented, the workforce needs to understand the need, reason and benefit from learning or adopting to a new technology; thereby the workforce is motivated to embrace the change.

Liang et al., (2015)'s study provides an interesting viewpoint on employees' interaction with information systems. They investigated employees' willingness to explore complex systems by stating that systems exploration enables employees to better integrate technology into their working environment and thereby increase productivity. Additionally, through Liang et al., (2015)'s study they found that system complexity, organisational environment and climate and task characteristics such as job autonomy are the main factors that simultaneously influence system exploration. The inverse effect, the lack of system exploration can potentially lead to

the opposite of productivity and performance, thus increase in possibility of errors and breaches.

Maalem Lahcen et al., (2020) also states that humans will make errors on even the best and most sophisticated systems. This provides support for Briggs et al., (n.d.)'s identification of the importance of the design and policies of a technology by stating that systems should rather be designed to minimise human error. It is thus clear information systems, and its underlying technology are secondary to the human operating it when comparing both of its impact on cybersecurity.

2.1.3.3 Organisational security culture

Some security factors are limited specifically to factors within the organisation's control, such as the security culture of the orginisation. Organisational security culture can be described as the collection of factors that influence and guide the workforces' behaviour that is in the best interest of an organisations information assets (CPNI, 2021). Additionally, organisational security culture aims to establish a strong security posture (Institute of Electrical and Electronics Engineers, 2014) and to ensure that actions are in accordance with information security policies (Luciano, 2014). These factors are known to be the beliefs, values, perceptions, attitudes and knowledge that is portrayed by and shared among the workforce which determines their behaviour (Chmura, 2016). Institute of Electrical and Electronics Engineers (2014) describes organisational security as a "human firewall", thus depicting the importance of the human role in information and data security. It is clear that organisational security culture plays an important role in understanding and determining human behaviour relating to data and information security as humans are widely regarded as the main source of security breaches.

The literature review suggests that the greatest contributing factors to a strong organisational security culture, is the physical, emotional, and intellectual wellbeing of the workforce, as well as the relationship of the workforce with the organisational management.

The physical wellbeing of employees refers to their physical state when working within their respective organisational environments. The physical state of employees is affected by various factors such as the working conditions, job type, salary, socialisation, commitment,

organisational climate and atmosphere within the organisation (Luciano, 2014). This physical state can have a significant impact on an individual's mental ability. Socialisation refers to collaboration and sharing of knowledge among colleagues and the evaluation of colleagues' opinions. Luciano (2014) highlights the importance of shared knowledge by stating that it can motivate the change in an individual's behaviour and potentially lead to the change in the behaviour of an organisation as a whole. A positive working environment and atmosphere contribute to an individual's perception of the security climate within an organisation. A positive climate can positively influence and reinforce an employee's emotional wellbeing such as their level of confidence, motivation, commitment as well as their sense of belonging. In turn, this can affect their behaviour towards information security. Working conditions that cause tiredness, fatigue, high levels of pressure, and low motivation lead to negative feelings such as anxiety, stress, discouragement and disinterest (Luciano, 2014). These negative feelings can have a detrimental effect on the information security posture as it affects and shapes the way employees behave and act towards information security best practices.

Luciano, (2014) describes an individual's knowledge by their level of familiarity with information systems and technology. Additionally, Luciano states that knowledge can be regarded as having any technical capability or general knowledge regarding information systems and technology that could be utilised to decrease the chance of compromises. Thus, having knowledge about certain threats, it can more easily be perceived by individuals. Individuals can thereby behave accordingly to avoid the chances of a breach happening.

Within information security, awareness is understood as the effort of the organisation to ensure the increase of results of security actions. The lack thereof is found to be one of the largest contributors to security breaches (Institute of Electrical and Electronics Engineers, 2014). Luciano (2014) states that awareness contributes significantly to security culture and posture, and that it could be enhanced through training. Through a qualitative study conducted by da Veiga et al., (2020), various findings from participants were made relating to awareness in security culture. Awareness is found to be the top trait of a strong security culture. Whereas the lack thereof being one of the root causes of data breaches, and as one of the main obstacles that organisations should focus on to establish a strong security culture. Among these findings, training and education are also found to be major contributing factors to increase ability, knowledge and awareness. Connolly et al., (2017) states that the goal of training and education is to provide employees with a guideline for acceptable usage and the outcomes associated with

the circumvention of rules. According to Deloitte, (2018) awareness training and workshops should be embedded into an organisation's strategy in order to support risk management. Shaw et al., (2009) explains in their study that the ability to detect threats, the accurate perception of threats, and the ability to predict and project threats are all traits that from part of individual's level of awareness. Therefore, a strong connection between the various characteristics of the individual's intellectual wellbeing is evident. An individual's level of awareness is strongly influenced by their knowledge regarding threats and safe practices, knowledge and ability could only be attained by adequate training and education on information security. According to Connolly et al., (2017), procedural security countermeasures such as security policies and procedures are important artifacts that also increase awareness. Additionally, Connolly et al., (2017) states that when employees are aware of the consequences of devious behaviour, it increases their understanding of the importance and significance of following organisational security procedures. Thus, it is clear that employees need justification for effort in order to follow policies and procedures.

The relationship between employees and employer is another important aspect of security culture, that ultimately relies on the management policies and procedures. Luciano (2014) states that the relationship among employees, managers and supervisors is crucial to the wellbeing of employees. This relationship creates a connection with the organisation with positive feelings, which ultimately contributes to their caretaking over their working activities. From the qualitative study of Chmura (2016), it was found that the encouragement and attitude of managers and their engagement with employees greatly impacts and determines the information security system of an organisation. All the various states of wellbeing of employees come down to the management aspect of organisational culture. Management policies determine the type of working environment and working conditions employees will be exposed to. Adequate management policies can establish a sense of trust and belonging among employees as well as influence their beliefs, values and perceptions. Consequently, it is important for employees to have their values and beliefs aligned with those set out by the organisation's culture in order to establish an environment where they can thrive in. Management procedures also influence the mental wellbeing and ability of employees as it is the responsibility of management to provide adequate training and education on threats, risks, and security in order to promote awareness and knowledge. A security-aware organisational culture will thus lead to a reduction in security risk and the misbehaviour of employees regarding information assets.

The concept of organisational management is a crucial factor to consider when referring to organisational security culture. The proper and adequate management of employees results in establishing a stronger security posture and ultimately, the management of potential security risks and threats.

2.1.3.4 The Behaviourist Theory

The *Behaviorist Theory*, also known as the *Behavioral Learning Theory*, was founded in 1913 and provides a perspective on behavioural learning through one's exposure to environmental stimuli (Dr McLeod, 2020). More specifically, this learning theory assumes that all behaviour is learned from the physical environment as it is observable. Behaviour results from the response to a stimulus and behaviourism does not take internal psychological processes into consideration to determine and study behaviour. However, the *Social Learning Theory* argues that both internal psychological processes as well as the behaviour learned from the physical environment influence an individual's behaviour (Western Governers University, 2020). Therefore, the Social Learning Theory requires a great amount of information about an individual's psychology, which may not be possible to obtain in an online survey for the purposes of his study. Additionally, exposure to cyber threats may manifest physically and act as an environmental stimulus, such an alert message or warning of the detection of a virus or malware or the reception of a phishing message or advertisement. Therefore, when an individual is confronted with a cyber threat, the individual is in fact exposed to an environmental stimulus. Thus, the Behavioral Learning Theory is deemed sufficient for the purposes of this study and can provide valuable insight into the understanding of human behaviour and their vulnerability to cyber threats. However, for future research the Social Learning Theory may be used to gain an even greater understanding of human behaviour when exposed to cyber threats. Within the analysis and methodology section an explanation will follow regarding the use of the Behavioral Learning Theory to aid in the development of survey questions. The survey questions will investigate stimuli-response behaviours in a digital environment. Therefore, the individual shall be questioned how they would respond to various digital threats. The answers to these questions shall provide insight to human behaviour when confronted with cyber threats. From these insights one can observe whether the individual is equipped with adequate knowledge, confidence, and skill to manage cyber threats. The answers will also indicate the security posture of the respondents.

2.2 Modern Digital Risk Management

Digital risks refer to unexpected or unwanted outcomes that may result from technology adoption or digital transformation (RSA, 2020). As modern organisations are undergoing rapid digital transformation, the more the reliance is on technology to safeguard digital assets as well as to evolve and sustain a competitive edge in the global economy. As a result, the potential exposure of digital assets and information to threats has become a great risk to organisations. Deloitte (2018) states that regardless of the risks that arise from digital transformation, organisations should not overlook the benefits and opportunities that arise as well. As digital transformation requires human employees and their capabilities to transform as well, the impact and role of the workforce should not be overlooked. In essence, regardless of the sophistication of the technology utilised, the behaviour and vulnerability of the human worker may represent the biggest digital risk.

At organisational level, risks can be described as any potential for a loss as a result of uncertainty (Spacey, 2015). Risks may also be described by the likelihood of an event's occurrence and the consequences associated with its outcome (Kure et al., 2018). When referring to digital risks, the focus is shifted to outcomes associated with the transformation, adoption and integration of technologies (RSA, 2020). Although the term risk and vulnerability has been used interchangeably, a fundamental difference exists. A vulnerability refers to the state of being exposed to danger and harm, while risk refers to the probability of which a vulnerability is prone to exploitation (Tungal, 2021). Within the domain of information and cybersecurity, a risk refers to a calculated assessment of a potential threats to security and vulnerabilities while a vulnerability is described as any gap or weakness that undermine an organisation's security posture (ThreatModeler, 2019). As it has been identified that organisations underestimate the impact and role of human-factor security within digital risk management. It is important to understand how digital risk management works and how organisations implement management strategies. Through this understanding and review of organisation digital risk management, it provides insight to how the impact of human-factor security is regarded within digital risk management. Additionally, this determines why human vulnerability is underestimated or overlooked.

2.2.1 Digital organisational risks

Business risks can be described as anything that prevents or hinders an organisation from achieving and maintaining its goals or targets (Corporate Finance Institute, 2021). Risks can come in many forms but are mainly classified as internal or external to an organisation. Some external risks are those which businesses willingly take to achieve a certain goal or to ensure organisational growth. These goals could include investing capital in new and growing business ventures without complete certainty that these upcoming companies will prevail. Other risks may stem from within an organisation, such as the vulnerability and susceptibility of the workforce that is related to normal, day-to-day working activities. Whether it is unintentional or due to a lack of knowledge or training, every time an employee interacts with an information system, potential risks can arise. As companies are transforming and become more reliant on digitised systems, the business risks, also known as "digital risks", presented by these systems must be alleviated, regulated and controlled. Digitised companies face an increased amount of IT security threats and data-related risks due to increasing technology adoption, which necessitate effective risk management strategies and models (BusinessTech, 2021). According to RSA (2020) as of 2020, roughly 60% of digital business will suffer as a result or lack of IT or security personnel to effectively manage digital risks. Modern technologies such as the Cloud and Internet of Things (IoT) bring a wide variety of risks to the table that are unrelated to the humans operating it. Through IoT, it creates a network of a great number of unsecured devices as in many cases the devices were not designed with security in mind (O'Flaherty, 2019). With the use of the Cloud, improper due diligence can cause third parties to form basis of attacks as organisations shift the responsibility and security priority to the hands of third-party vendors (O'Flaherty, 2019). Although these technologies and its underlying risks are internally related to business operations, the impact of the human role in the interaction and management of these technologies is still overlooked. Digital and security risks can also have a significant impact on other organisational risks such as compliance, reputational and financial risks (Capodagli, n.d.).

De Oliveira (2020) names 7 main risks that digital risks consist of, namely: Cybersecurity Risk, Compliance Risk, Automation Risk, Workforce Risk, Third Party Risk, Resiliency Risk and Data Privacy Risk. Workforce Risk are explained as any risk caused directly by an employee such as lack of skill or high employee turnover.

Mohammed & Mohammed (2017) identifies two main sources of security management risks namely insider threats, and the lack of due diligence. Insider threats are risks presented by anybody with malicious intent from within the organization. The lack of due diligence occurs when a person is negligent with regards to security protocols and policies interacting with information systems.

According to the Institute of International Finance and (McKinsey & Company, 2017) as of 2017, two main challenges that risk managers struggle with is IT legacy systems and organisational culture, thus referring to the discussion in section 2.1.3.3.

According to Costello (2019) risk management involves a strategy that is integrated into every organisational level and more specifically, a set of processes and practices that are driven by a security-aware culture and its supporting technologies.

A new digital threat that has made its way to the attention of major banks and e-commerce enterprises is the risk attached to a term called "screen-scraping" of online transactions. The awareness of transactional screen scraping started getting attention from many news publishers as early as 2020 and is currently still making its rounds (Gardiner, 2021). Screen scraping in e-commerce occurs when a third-party organisation mirrors a login portal with false equivalency to those of banking application. Thereby they can capture consumer login credentials while they unwittingly disclose this information (Gardiner, 2021). The third-party organisations can thereafter access a user's banking account, with the banking company unable to detect the difference between the actual user logging in or a third-party user/organisation (Gardiner, 2021). The risk associated with this method of payment, widely known as EFT‘s, is that it exposes a user's personal information to the possibility of fraud, financial crime and data privacy (BusinessTech, 2021), while the user remains completely unaware. The same scenario applies to organisation who authorise banking, credentials and information access to a third-party. Although the third-party may not have malicious intent, the risk of exposure yet remains. This treat and risk is especially relevant to this study and the current digital industry as digitalisation is becoming the norm for services and transactions.

2.2.2 The "human" side of risk management

The human employee has a footprint and role in every level and facet of an organization. Therefore, to establish a cohesive security posture, a joint input from each employee is required. Many studies highlight the importance that security awareness and training has on an organisations ability to prevent, decrease, or mitigate security risks. NRECA (2011) provides a cyber-security mitigation plan which outlines that organisation needs to ensure that new employee hires are trustworthy, that there is ongoing security training for all employees, especially those who have access to sensitive and protected assets. Lastly, the mitigation plan ensures that employees are only granted the level of access and privileges needed to perform their jobs. Furthermore, NRECA (2011) states that a cybersecurity training plan should provide education that enables employees to make proper use of sensitive and critical assets, the ability to handle critical information, the ability to recover or reestablish critical assets in the event of a security breach or incident. Lastly, through training employees should be able to follow policies, procedures and access controls that are specially developed for security assets.

Kure et al., (2018) defines any person who interact with the system as "actors" and states that it is the responsibility and role of actors to ensure that risks are kept to a minimum. These actors include non-IT, management or security personnel. RSA (2020) states that in order to effectively manage risks, risk management and security teams must work in cohesion, thus putting emphasis on higher level management. Although the impact of management on the workforce is not thoroughly described, they still identify the workforce as being a contributor to digital risk. The focus is placed on factors such as access policies and role authentication, which are authorised and implemented by management. According to Luciano (2014) studies have shown that employee security is in fact very difficult to audit as a result of individuals' personalities and perception that causes them to react and behave differently. This emphasises the complexity and importance of adequate risk management.

RSA (2020) provides a report on digital risk management and outlines eight different types of digital risks modern organisations are faced with. As the Workforce/Talent risk can be seen as directly related to the human side of risk management, the role that humans play in the other digital risks can clearly be derived. The other seven risks are outlined as *Cybersecurity*, *Cloud*, *Compliance*, *Third-Party Risk*, *Process Automation*, *Resiliency* and lastly, *Data Privacy*. Deloitte (2018) and RSA (2020) highlights digital resiliency as a crucial factor in risk

management due to organisations' high dependence on technology. Deloitte (2018) proposes an actual purchasable risk management framework that focuses on 10 risk areas that an organisation may be potentially exposed to. These 10 risk areas are *Technology*, *Cyber*, *Strategic*, *Operations*, *Data Leakage*, *Third Party*, *Privacy*, *Forensics*, *Regulatory* and *Resilience.* Similar as with the RSA (2020)'s report, by studying Deloitte (2018)'s various risk areas there can be clearly derived that the human employee has a significant impact on each of the risk areas. RSA, (2020) highlights Cyber incidents, third party governance, Data Privacy, Resiliency as their four main risk areas. There thus exists a strong relation between higher level management and the proficiency and capabilities of the workforce. As seen in multiple studies, technology and its use and the dependency and complexity play a big role in risk management through the workforces' interaction with it.

2.2.3 Risk management and assessment insight

The goal of the following subsections is to gain an understanding of risk management models presented by research papers, organisational reports, and web articles relevant to this field of study. Additionally, there will be investigated what are the main factors that risk management models consist of and what are the shortcomings identified among these models. In the last section, risk assessment formulas and equations are discussed. These risk assessment formulas and equations shall assist in developing a risk assessment formula which is appropriate for this study. This formula will then be utilised in the risk assessment of threats identified in Chapter 4.

2.2.3.1 Models and frameworks overview

The literature suggests that some papers provide theoretical insight into risk management by providing step by step guides, while others present risk identification and assessment formulas as part of their model or framework. The rest of this subsection will be a review of these papers and reports.

The literature provides insights on risk management in organisations as a whole, and with a focus on specifically digitised risk management. There is suggested that management models and frameworks that could be applied in different contexts or industries, such as construction,

finances, banking, and within the government. The focus of these management models and frameworks is on minimising the risk caused by cyber related threats.

Limba et al., (2017) presents a multidimensional cybersecurity risk management model that could improve the cyber security and critical infrastructure of any organisation. The model consists of six core factors that are essential for establishing a strong cyber security posture. These six core factors are identified as legal regulation, good governance, risk management, security culture, technology management and incident management. Limba et al., (2017) also states that an organisation is just as vulnerable as the workforce and highlights the importance of having a knowledgeable and skillful workforce that can learn and defend against various attacks. Just as it was identifiable where the workforce plays a role in many of the risk areas provided in the report of Deloitte (2018), it is identifiable that the workforce plays a significant role in most of the different core factors present in the study of Limba et al., (2017).

Wawrzyniak (2006), proposes a risk assessment model that could aid in risk management at different organisational levels. Although Patel & Zaveri (2010)'s study focuses on risk management within industrial plants, insight could be drawn to the probability of attacks on an information system as well as how to calculate potential loss because of various attacks. Wawrzyniak (2006) identifies the main problems with quantitative and qualitative risk analysis as being too difficult to use or understand by managers in organisations. Thereby, a quantitative analysis model that incorporates both easy usability and comprehensiveness is proposed. Model et al., (2018) has provided a report that aids government agencies with an implementation model to address risk management and cybersecurity needs as well as how to approach various cyber security challenges. NRECA (2011) provides a comprehensive cybersecurity mitigation plan through a theoretical approach. Studies and reports like these are useful to aid managers in various industries to understand and design a systematic approach to risk management and to prepare a risk mitigation, prevention, or recovery plan. However, the impact, risk and threats posed by the workers itself is not entirely brought into question by Patel & Zaveri (2010), Wawrzyniak (2006) or Model et al., (2018). McKinsey & Company (2017), RSA (2020) and Deloitte (2018) have all provided comprehensive and detailed reports on the management of risk within the digital era. McKinsey & Company (2017) report aids organisations specifically in the banking and finance thechnology industry to establish a short- and long-term digital risk management plan. RSA (2020) has provided a report which identifies and discusses the eight major types of digital risks with data privacy being the most common

risk faced by organisations. Deloitte (2018) provided a report where they identify major risk areas within digital environments and explain how their framework is utilised to manage risk in these areas.

The following papers suggests quantitive approaches to risk assessment.

Patel & Zaveri (2010) proposes a mathematical risk assessment model that calculates the financial losses and impact caused by cyber-attacks on information systems specifically within industrial plants. The model can also be used by organisations for cost/benefit analysis of the acquisition of hardware and software.

Kure et al., (2018) provides an in-depth risk management strategy by presenting equations for the calculation of asset criticality, asset vulnerability impact, risk assessment, the impact of security-attack scenario, risk criticality level as well as provide a vulnerability identification checklist.

Bojanc & Jerman-Blažič (2013) presents a model that calculates the probability of a security incident occurring, financial loss due to a security incident as well a calculation of all the factors that determines risk. Additionally, their model assesses the financial return on security measures. Bojanc & Jerman-Blažič (2013) also presents a diagram that models a risk management process which includes the logical steps to be taken in order to assess and determine a type of risk. Thereby there can be decided on what counter measures or actions that should be taken.

GOVERNANCE & STANDARDS DIVISION (2017) provides an in-depth risk management framework that outlines and guides each step of the risk assessment process. The framework includes formulas and provides a comprehensive list of the threats and vulnerabilities that potentially has an impact and hinders an organisation ability to achieve its goals and objectives.

Ao et al., (2008) provides a review of various qualitative as well quantitative methods that could be utilised to conduct an IT risk analysis. Ao et al., (2008) also describes what factors should be considered and includes when conducting an IT risk analysis. The analysis includes the assessment of probability, frequency, consequences as well as an analysis of susceptibility, protection, and the evaluation of the impact on various resources with its underlying formulas.

NRECA (2011) outlines in their report a five-step process for the assessment and mitigation of security risks. The five steps include system characterisation, threat identification, vulnerability identification, risk assessment, and control recommendations. NRECA (2011) also describes security risks by belonging to one of three categories: people and policy, process, or technology. Although the report does not provide any practical formulas for risk assessment it provides significant insight to the critical factors to consider and should be included in a risk assessment and mitigation plan.

These quantitive approaches to risk assessment suggested above shall be reviewed in the following subsection.

2.2.3.2 Review of risk assessment formulas

This subsection will review various risk assessment formulas and calculations provided by existing literature in order to gain a wider perspective on the variables that are considered and included in risk assessment strategies. These formulas typically include the factors that are used to calculate and determine the impact of risk posed by potential threats and the probability that the threat will occur. Finally, a risk assessment formula will be proposed which considers the factors and variables used in the different formulas presented by the existing literature that follows below. This formula will then be used to conduct risk assessment in Chapter 4.

NRECA (2011) describes in their report that risk level or severity should be derived from the function of its likelihood of occurrence and impact on an organisation's goals. This forms the foundation on which other studies also measure risk severity, thus implying the following formula:

$$RISK = LIKELIHOOD \times IMPACT \qquad \text{Equation 1}$$

NRECA (2011) proposes that the expected likelihood and expected impact should be measured on a five-level scale or on a scale between *High*, *Medium* or *Low*. The expected likelihood should be determined on the nature of the identified vulnerability, the capability of the threat, and the effectiveness and strength of existing controls. The expected impact should be measured by the potential damage to a system, data or to an organisational goal. Additionally,

NRECA (2011) states that the understanding of an event helps with the development of a risk mitigation strategy starts firstly with the combination of actions such as the detection of an occurrence, reducing the likelihood of the occurrence, improved recoverability from the occurrence, or transferal of the risk. Secondly, the following factors can help guide the development of a strategy: determining the nature of the issue such as compliance, privacy, technical, other, determining whether the mitigation deals will people, processes or technology, determining whether the risk is acceptable to the organisation and lastly, determining whether the cost of completely remediating the risk is justifiable.

GOVERNANCE & STANDARDS DIVISION (2017) describes risk determination by the combination of the risk posed by the probability of the occurrence and the loss of *confidentiality*, loss of *availability* and loss of *integrity*. Thus, the following formula can be derived:

$$Average\ Risk = \frac{(Impact\ \% \times Probability\ \%\ of\ Confidentiality)}{3} + \frac{(Impact\ \% \times Probability\ \%\ of\ Availability)}{3} + \frac{(Impact\ \% \times Probability\ \%\ of\ Integrity)}{3} \quad \text{Equation 2}$$

However, GOVERNANCE & STANDARDS DIVISION (2017) determines the combined risk (CR) by including the worst-case scenario into the calculation. Thus, the complete formula is:

$$Combined\ Risk = \frac{(Average\ Risk + Worst\ Case)}{2} \quad \text{Equation 3}$$

The worst-case risks represent the highest risk value among the loss of confidentiality, availability, and integrity.

The following factors should be considered when determining the probability of an occurrence: The source, motivation and capability of the threat, the nature of the vulnerability, and the effectiveness of existing controls. Threat impact is determined by the sensitivity of the targeted assets, and it's required level of protection. GOVERNANCE & STANDARDS DIVISION (2017) rates the impact of breaches on the scale of 1 – 5 with the following five descriptions starting from one to five: insignificant, minor, moderate, major, catastrophic. The following

table is also provided that categorises the expected probability (or likelihood) of an occurrence with its description based on five rating levels:

Rating	Description	Probability of Occurrence
1	Rare	Highly unlikely, but it may occur in exceptional circumstances. It could happen, but probably never will.
2	Unlikely	Not expected, but there's a slight possibility it may occur at some time.
3	Possible	The event might occur at some time as there is a history of casual occurrence at the similar institutions.
4	Likely	There is a strong possibility the event will occur as there is a history of frequent occurrence at similar institutions.
5	Almost Certain	Very likely. The event is expected to occur in most circumstances as there is a history of regular occurrence at similar institutions.

Figure 2.2: Rating the probability of the occurrence of threats (GOVERNANCE & STANDARDS DIVISION, 2017)

Utilising Equation 1, GOVERNANCE & STANDARDS DIVISION, (2017) derives a risk impact matrix, which can be seen in Figure 2.3. This risk impact matrix can be used to classify the severity of risks in terms of expected likelihood and expected impact. For the formulation of the matrix, the likelihood and impact are rated on a scale of one to five. The expected likelihood is rated according to Figure 2.2. The expected impact is also rated on a scale of one to five, with the following five descriptions starting from one to five: insignificant, minor, moderate, major, catastrophic. Utilizing Equation 1, the risk can be quantified as the likelihood rating multiplied by the impact rating. Therefore, a risk with a low likelihood rating and a low impact rating will result in a risk that is classified as a low severity risk. Conversely, a risk with

a high likelihood rating and a high impact rating will result in a risk that is classified as a high severity risk. The Risk Impact Matrix shown in Figure 2.3 visualises the low severity risks in dark green, moderate severity risks in yellow, and high severity risks in dark red.

		Impact				
		1	2	3	4	5
Likelihood	1	1	2	3	4	5
	2	2	4	6	8	10
	3	3	6	9	12	15
	4	4	8	12	16	20
	5	5	10	15	20	25

Figure 2.3: Risk Impact Matrix (GOVERNANCE & STANDARDS DIVISION, 2017)

Ao et al., (2008) provides a comprehensive study investigating both qualitative and quantitative IT risk analysis methods to determine their advantages and disadvantages.

Risk Analysis	Quantitative methods	Qualitative methods
Chosen advantages	– They allow for definition of consequences of incidents occurrence in quantitative way, what facilitates realization of costs and benefits analysis during selection of protections. – They give more accurate image of risk.	– It allows for putting in order risks according to priority. – It allows for determination of areas of greater risk in a short time and without bigger expenditures. – Analysis is relatively easy and cheap.
Chosen disadvantages	– Quantitative measures depend on the scope and accuracy of defines measurement scale. – Results of analysis may be not precise and even confusing. – Normal methods must be enriched in qualitative description (in the form of comment, interpretation). – Analysis conducted with application of those methods is generally more expensive, demanding greater experience and advanced tools.	– It does not allow for determination of probabilities and results using numerical measures. – Costs-benefits analysis is more difficult during selection of protections. – Achieved results have general character, approximate etc.

Figure 2.4: Advantages and disadvantages of quantitative and qualitative risk analysis methods (Ao et al., 2008)

Ao et al., (2008) provides a formula for the calculation of risk assessment in Figure 2.5.

$$R = P \times W \text{ and } P = F \times V$$

where:
R – Risk value,
P – Probability or predicted number of incident occurrence causing loss of assets value in defined period ,
W – Value of loss – predicted medium loss of assets value, as a result of single incident occurrence,
F – Frequency of threat occurrence,
V – Susceptibility of Information system on (or its element) a threat; it is the measure of probability of usage of specified susceptibility by a given threat.

Figure 2.5: Risk assessment formula (Ao et al., 2008)

Kure et al., (2018) defines risk based on levels that is determined by the likelihood and impact of vulnerability for a given scenario, thus providing the following formula:

$$RL = L(S) \times I \qquad \text{Equation 4}$$

Where:

RL - Risk Level
L - Likelihood
S - Specific scenario
I - Impact of vulnerability

Additionally, Kure et al., (2018) provides a risk category level table depicting the risk level based on certain score intervals and description of each level, as seen in Figure 2.6.

Risk Level	Score	Description
Extreme	10.0–8.00	The risk level is extremely critical and requires the implementation of the control measures to mitigate risk almost immediately. The risk level is extremely critical when both the likelihood and the impact of the risk event is extreme. Could result in serious damage that could obstruct the operations of the organization.
High	7.99–6.00	The risk level is highly critical and requires the implementation of the control measures for mitigating risk that has to be immediately within a short time frame. The risk impact is highly critical when both the likelihood and impact of the risk event are extreme and/or high. Expected to have a serious impact on the organization's reputation.
Medium	5.99–4.00	The risk level implies that the risk has an adversarial effect on the organization and effective actions need to be applied to the contingency plan of the organization and within a specific period of time. It is likely to result in a short-term disruption of the organization's services.
Low	3.99–2.00	The risk level from the risk event requires the organization to take effective actions and may require the need for a new contingency plan as well as corrective measures.
Very low	1.99–1.00	This risk level indicates that a corrective measure needs to be implemented and a contingency plan needs to be developed.

Figure 2.6: Score table for different levels of risk (Kure et al., 2018)

Lastly, according to Kure et al., (2018) threats and vulnerabilities have three underlying properties: impact, type, and weight score.

2.2.4 Section conclusion

From the review of literature in this section many limitations with regards to the impact of human behaviour in organisational risk management were identified. Most papers and reports that were reviewed are limited only to the acknowledgement of the role and impact of humans in risk management. Its impact and significance are thus a vaguely explored area. Human behaviour and vulnerability to cyber/digital threat are found to be influenced by various internal (cognitive and psychological) and external factors (environment). With regards to digital risk management, many papers propose formulas and frameworks for risk identification and assessment, but rarely implement the frameworks on authentic datasets. A general focus and concern found among many papers, reports and websites is an organisations resilience in the modern digital world. As organisations continue to become more digitised and the more sensitive customer data processed and stored, the higher the risk of exposure and security compromises. It is thereby important for organisations to be prepared for the inevitability of threats and to be able to withstand and recover from a breach. It is evident that only a single breach may lead to repercussions that an organisation could not recover from.

Chapter 3

Methodology

The aim of this chapter is to describe the methodology used to investigate the behaviour of employees when interacting with information systems. The degree of security or digital risk awareness of these employees working in digitised companies will be determined. In addition, the level of risk and security awareness and readiness from the organisation itself will be determined. Empirical data for this study will be collected in the form of surveys distributed to employees within digitised companies. An invitation to the survey will be sent to participants within digitised organisations through word of mouth and a social media invitation (LinkedIn). The research design for the qualitative study will be described. Additionally, the procedure of how participants were chosen and recruited will be discussed. Lastly, the data collection process, storage and management will be described.

3.1 Design

A quantitative survey approach can be seen in the study of Ani et al., (2019), which aims to quantify the security capabilities and knowledge of the workforce. Through the quantitative analysis on a target sample, Ani et al., (2019) quantifies the proficiency of employees to interact with and manage digital risks. Their proficiency was quantified based on their level of knowledge, skill, and biases. Through Ani et al., (2019)'s quantification approach, the individuals displaying the lowest proficiency within the workforce or group could be identified. As a result of the effectiveness of this survey approach conducted by Ani et al., (2019), a similar survey approach was selected as the main method of data collection for this study.

The survey will consist of three sections. The first section (Section A) of the survey will concern questions that estimate the overall security and risk awareness from participants. This section will consist of multiple-choice questions, mostly in the form of Likert-scales. The second section (Section B) of the survey will consist of questions that utilise The Behavioral Learning Theory to investigate the stimulus-response behaviours when employees interact with information systems. This section focusses on how the participants respond when exposed to certain stimuli, for example, how a participant would possibly respond when a virus warning

notification appears on their workstation computer. The various responses or reactions to this warning notification could potentially introduce many threats to the organisation. In this second section, utilising The Behaviourist Learning Theory, the participants will be prompted to type their responses towards a certain stimulus in a provided text box. Thereby their intended actions are depicted. The data collected from this section will aid in qualitative analysis of the potential threats that may arise from risky behaviour portrayed by participants.

A risk identification and assessment formula, as reviewed in the literature review, will be applied to the stimuli-response scenarios. The various responses to each question will be discussed based on their severity and potential damage that it could cause to the organisation. The degree of proficiency, knowledge and awareness of the participants will also be derived from their responses to various stimuli. After the risk identification and assessment has been applied, a summarised table of results will be produced. Additionally, appropriate responses to each identified risk will be provided.

The third section (Section C) will aid the qualitative analysis to investigate personal biases and perceptions relating to participants' own posture and abilities in cyber security. This section will also consist of questions relating to the security culture within organisations. The aim is to investigate the overall level of security and threat awareness and what practices they implement to establish a strong security posture among the workforce.

3.1.1 Survey Section A: Overall security and risk awareness

The purpose of this section is to investigate the overall level of awareness regarding common security measures and practices as well as common risks and threats related to human-factor security. Likert-scales with varying scales depending on the question will be used to catagorise participants' answers. An example question related to password management:

How regularly do you change your passwords? Select the answer that best matches your actual behaviour.

1. *Weekly*
2. *Monthly*
3. *Once every 2-3 months*

4. *Once every 3-6 months*
5. *Yearly*
6. *Never*

This section is divided into four subsections: Organisation related questions, Password management, Protection of devices and lastly, Overall technology proficiency and awareness. In total, this section consists of 19 short multiple-choice questions.

3.1.2 Survey Section B: The Behavioural Learning Theory

Section B of the survey utilises the Behavioural Learning Theory. The questions in this section are designed to emulate a stimuli-response environment. The participant is questioned on how they would respond when faced with various cyber threats. The answers shall give an indication of the level of skill, proficiency, and confidence with which the respondents are able to respond to cyber threats. Survey Section B is further divided into two subsections. The subsections are Section B1, focusing on actions and behaviour within the organization, and Section B2, focusing on actions and behaviour outside the organisation.

3.1.2.1 Actions and behaviour within the organisation (Section B1)

The purpose of this section is to gain a cumulative understanding of how people react/respond when faced with certain scenarios in their interaction with technology at the workplace. Interactions with information systems at the workplace at may cause risks or vulnerabilities for an organisation. Such interactions with technology include logging in to the company portal or information system, working on the company local computer or simply connecting to company Wi-Fi. With the multiple scenario questions provided in this section, participants will be able to input their response to certain questions/stimuli within the text boxes provided. In total, this subsection consists of eight "type your own answer" questions.

3.1.2.2 Actions and behaviour outside the organisation (Section B2)

This section shares the same goal as section B2, but with the scenarios focusing on the interaction with technology stemming offsite (outside the organization). Such interactions with technology or behaviour could indirectly have a potential negative impact on the organisation. Examples of such interactions include file sharing from offsite networks to onsite portals or

infecting an electronic device from a public network and then connecting that device to an onsite network. All these types of actions are potential vulnerabilities for an organisation that could easily be exploited by people with malicious intent. In total, this subsection consists of five "type your own answer" questions.

3.1.3 Survey Section C

The purpose of this section is to add an additional qualitative aspect to the study to gain an understanding of the participants' personal security posture. The questions are centered around participants' perception biases relating to the importance of security practices. Participants are also questioned on their own perception of the security culture and requirements within their company. These questions will require participants to type their answers in the text boxes provided, thus allowing the gathering of more personalised and unique answers. In total, this section consists of nine short "type your own answer" questions.

3.2 Qualitative study

As a result of the nature of the questions set up in the survey, only a qualitative study will be conducted on the data set. However, the statistical programming language "R" has been used to transform the dataset to create a visualisation of the distribution of data with relation to age and gender groups.

The goal of the qualitative study is to gain insight and an understanding of the types of threats and risks that arise from the behaviour and activities of people who rely on technology in their everyday life. This includes work-related and non-work-related activities. Additionally, this study investigates people's understanding of digital risks and security behaviour as well as how they perceive the security culture within their own organisation. An open source qualitative data analysis tool, "Taguette" was chosen as the tool to conduct the qualitative analysis with, as this software allows for the grouping an analysis of themes within a set of qualitative data.

The Behavioural Learning Theory was utilised to aid the qualitative study by setting up questions (Survey Section B) that emulate a stimuli-response environment. Thereby, the survey participants' responses when exposed to environmental stimuli, in this case digital threats, could be analysed to gain insight into the triggers and causes of certain behaviours.

3.2 Participants & procedure

3.3.1 Participants

For the target audience of the survey for the qualitative study, any person who forms part of the working class in South Africa who works in the IT industry or related field were targeted. This includes any person who considers themselves heavily dependent on technology in order to their day-to-day working activities. Thus, people who work in digitised (technology-based) organisations are the main target. In terms of participant demographics, there is no specific age requirement, but the participant must be part of the labour market, thus assuming that all participants will be older than the age of 18. Participants were however prompted to provide their age to identify whether there are different levels of threat and risk awareness, perception and behaviour among different age groups. Participants' gender was prompted in order to identify any potential differences in awareness and behaviour among gender groups. Lastly, participants were prompted to specify their current job/role in the labour market. Through the specification of different job roles and titles, there was aimed to determine the general level of threat awareness and ability between different IT or related industries. These general demographic variables serve as a means to identify trends in behaviour and patterns among different groups in the dataset. It is expected that there is no significant difference among gender groupings, but perhaps in age groupings.

3.3.2 Methods of recruitment and procedure

The recruitment of the above-mentioned participants relied on two methods of spreading of the survey. Firstly, a post on LinkedIn inviting any person who consider themself technology dependent in their everyday working life to participate. Secondly, by the spreading of the survey through word of mouth. This consisted of an invitation to the survey through Emails as well as personal messaging applications. A R500 gift voucher was added as an additional incentive to participate which was given to a randomly selected participant who added a valid Email address at the end of survey. Providing an Email address was optional for participants and did not affect the submission of the answers to the survey. The Email served as a way for the gift voucher to be able to be sent to the lucky winner of the voucher.

3.4 Data collection

Before any participation in the survey is made possible, participants were prompted to provide acknowledgement of the purpose and goal of the survey as well as indicate their consent to participate. For those who do not indicate acknowledgement and consent, the electronic survey was unable to start with the questions, ensuring that ethical requirements were met.

The survey was designed, created, and managed directly from Google Forms. All data collected from the surveys was stored and secured on Google Forms and exported for analysis. A target with a minimum of 50 respondents was set to ensure diversity and accuracy in results as well as increasing the scope of unique answers.

The anonymity of the survey responses assured the minimisation of personal biases that may be captured as a result of the open-ended questions.

Chapter 4

Data Analysis

4.1 Introduction

After the survey was closed to participation, a total of 58 responses were captured. Out of the 58 responses who gave their consent to participate, three participants did not provide any background information in the introduction of the survey with regards to age, gender and job/role specification. For content related questions, out of the 58 respondents, some questions yielded a total response amount as low as 51. This may be as a result of some respondents willingly choosing not to answer the questions or perhaps did not understand the question and skipped it. The answering of all questions was voluntary. Two participants did not complete the survey and only provided an Email address for the lucky draw and one participant for half of the questions provided non usable answers. These three responses were thus purposefully rejected from the dataset where applicable. For the purpose of the analysis, the total amount of responses per question individually will be used as the base on which each question's analysis will be conducted on, thus not affecting the entire dataset due to missing responses.

The purpose of the data analysis in this Chapter is to answer Research Questions 3 to 5, as previously presented in the Section 1.3 of Chapter 1:

- Are modern digitised organisations aware of the impact and vulnerability of the workforce related to cyber threats? (RQ 3)
- Do digitised companies implement risk management strategies that cater for or mitigate potential threats caused by the workforce? (RQ 4)
- Does the average worker possess the level of knowledge, skill and risk awareness in order to implement adequate security measures in their day-to-day activities within organisations? (RQ 5)

4.2 Descriptive Analysis

This section presents the descriptive analytics from the insights gained from the survey. The demographics of the sample shall be presented. Additionally, the descriptive analysis shall be provided for the sample's awareness and mindfulness, risk identification and assessment, as well as their personal and orginisational related perceptions.

4.2.1 Demographics

Of the 56 total survey respondents, 28 (50%) were male, 28 (50%) were female thus displaying an equal distribution. Figure 4.1 displays the Gender distribution for each age category between ages of 20 and 60 in intervals of five. Pre-assumptions are made that gender will not show variance in answers in terms of security posture, risk and threat awareness.

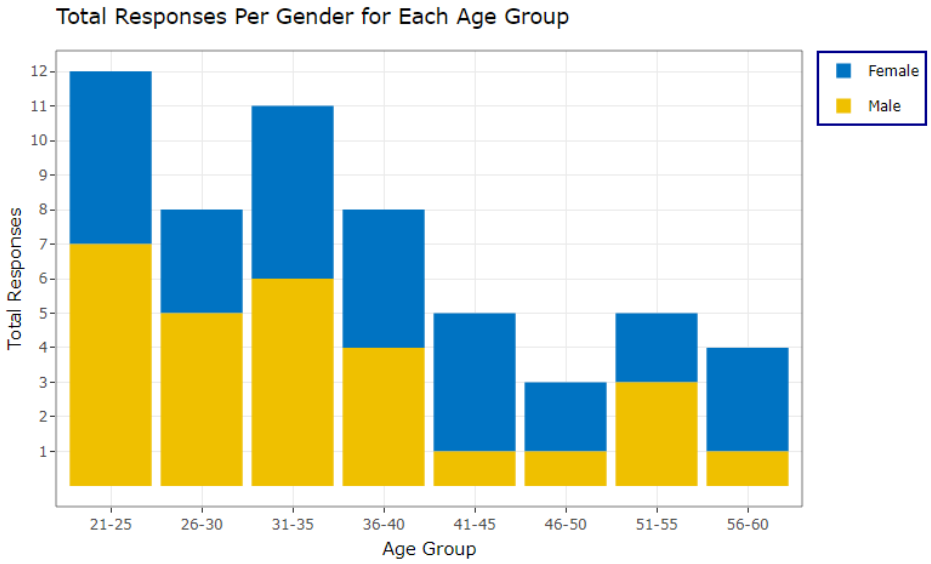

Figure 4.1: Total responses per age group

The median age is 36 and 39 (69.6%) responses from the pool of participants are younger than the age of 41. Consequently, as evident in the figure 4.1 above, the distribution is more biased towards participants with the age of younger than 41. As a result of the variance in the age intervals, age will not be used as a factor for measuring the results of the survey and serve as a limitation.

It is interesting to observe that the distribution in the age of female respondents appears to be approximately uniform, whereas the distribution in the age of male respondents appears to be slightly skewed towards a younger age. This observation can be seen in Figure 4.1.

4.2.2 Awareness and mindfulness

To formulate a perception and gain insight into the general level of awareness and mindfulness towards digital threats among the pool of participants, the survey employed a series of multiple-choice questions (Section A). Multiple choice questions were chosen as method of data capture for this section as it will allow to differentiate between groups of respondents based on the total amount of chosen answer per question. The differentiation will provide an estimation of the general level of mindfulness toward security risks and threats that already exist among the workforce (pool of respondents). In the case of this study, the pool of respondents serves as a general representation of the actual workforce. These questions revolved around four main groups: Organisational related questions, Password Management, Protection of Devices and lastly, Overall Technology proficiency and awareness. These four groups were formulated as it encompasses a wide variety of factors and influences that are applicable to the modern-day employee where technology is prominent in every aspect of one's life. The full list of survey questions for each section can be seen in Appendix A.

The *Organisational related questions* subsection investigated participants' trust in their organisation with relation to the safeguarding of their personal information (*Q2). Additionally, this refers to the usability and usage of the organisations information system and technology (*Q3-Q6). 89.3% (50) of respondents use a login system through which they are enabled to do their work. This corresponds to the modern digitised organistion where it is visible that many activities are conducted and safeguarded through an organisaion-wide portal or system. Participants show a high level of trust in the organisation's system with regards to safekeeping their personal information as the majority (40) stated that they fully trust their organisation (*Q2). Gender does not influence the level of trust in the organisation as seen in Figure 4.2.

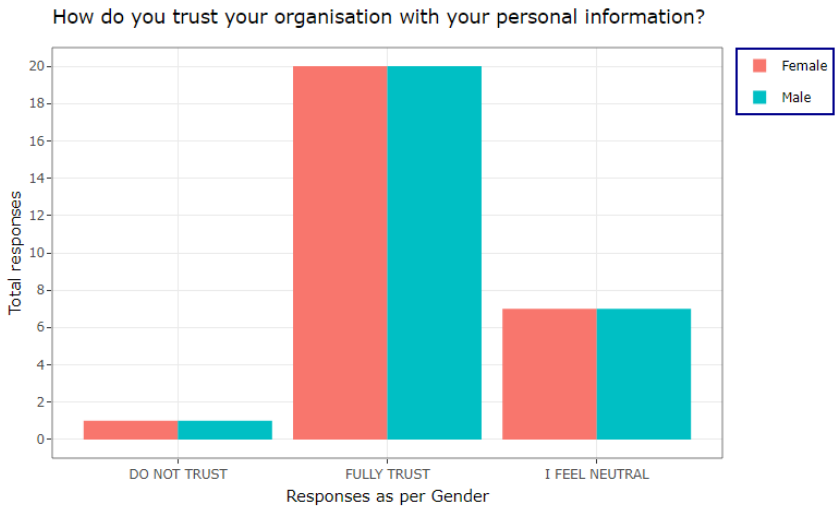

Figure 4.2: Organisational trust per gender group

When asked about their perception of the safety of their interaction with technology on the organisational information system (*Q3), 37 (66,1%) respondents show confidence in the safety of their action. Whilst 16 (28.6%) felt neutral and 3 (5,4%) felt unsure. When observing the gender distribution in figure 4.3, for those who chose "VERY SAFE", female respondents show a higher confidence in their interaction, while from those who selected "NEUTRAL" male respondents appear to the frontrunner.

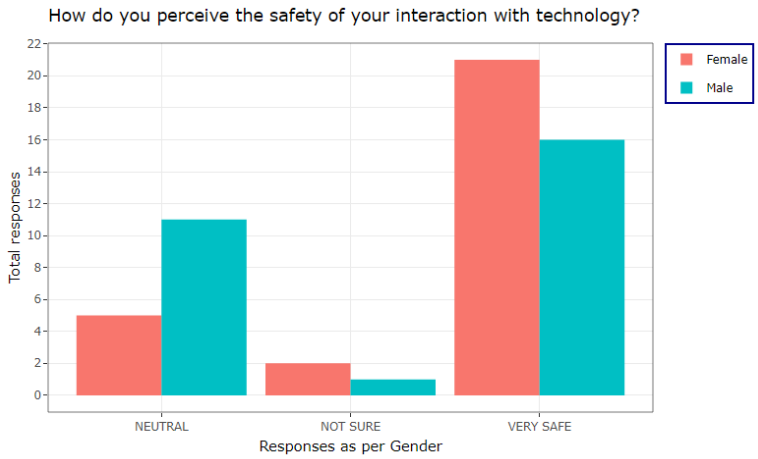

Figure 4.3: Gender group perception of technology safety usage

34 (60.7%) respondents indicated that they make use of personal electronic devices on their organisations networks (*Q4), while 22 (39.3%) indicated that they do not. From the 56 respondents, 47 (83.9%) are allowed to take their company device offsite while 9 (16.1%) are not allowed (*Q6).

When participants were asked about the usability of their organisation's information system (*Q5), 32 (57.1%) indicated that the system is very easy to use, for 20 (35,7%) the system is somewhat easy to use. Only four (7.1%) indicated that they find the system sometimes difficult to use. None of the respondents indicated that they struggle to use the system. For all three answers to this question, the responses per gender are distributed evenly. In total 42.8% of respondents do not find their organisation’s information system very easy to use. This finding corresponds to the discussion in Section 2.1.3.2 within the literature review. Many studies have found system complexity and usability as a contributing factor that leads mistakes and errors (Delaney & Delaney, 2015; Furnell, 2005; Liang et al., 2015).

With regards to the *Password management* subsection, respondents show diversity in their answers for how regularly passwords are updated or changed (*Q7).

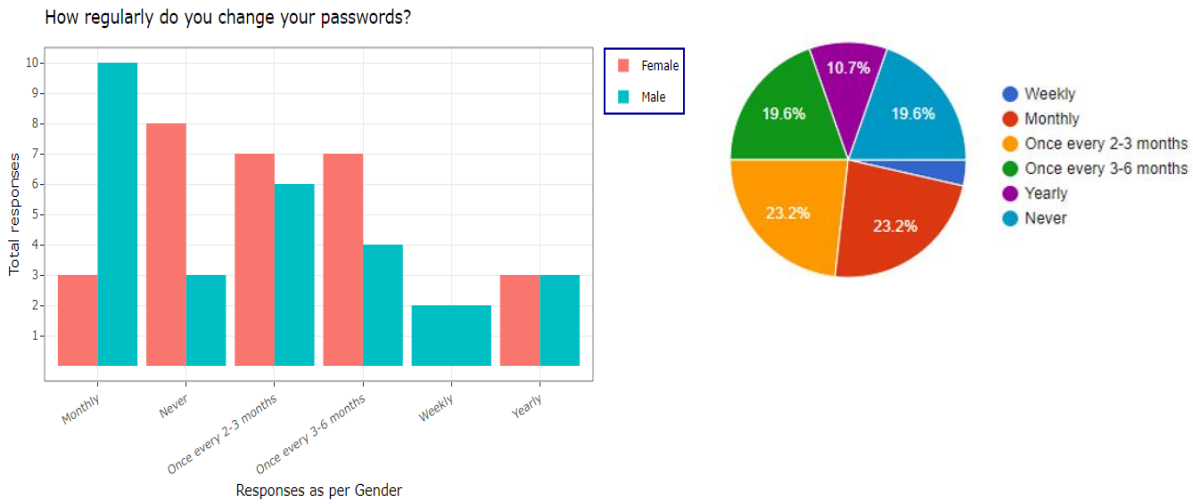

Figure 4.4: Gender group password change frequency

Figure 4.4 indicates that only two respondents stated that they change their password on a weekly basis and both "Monthly" and "Once every 2-3 months" have 13 responses respectively. According to Johnson, (2020), security experts claim that a password should be changed at least every three months. Surprisingly, 11 respondents (19.6%) indicated that they never change their passwords. It is important to note that no female respondents for this survey change their passwords weekly. However, two male respondents indicated that they change their passwords weekly.

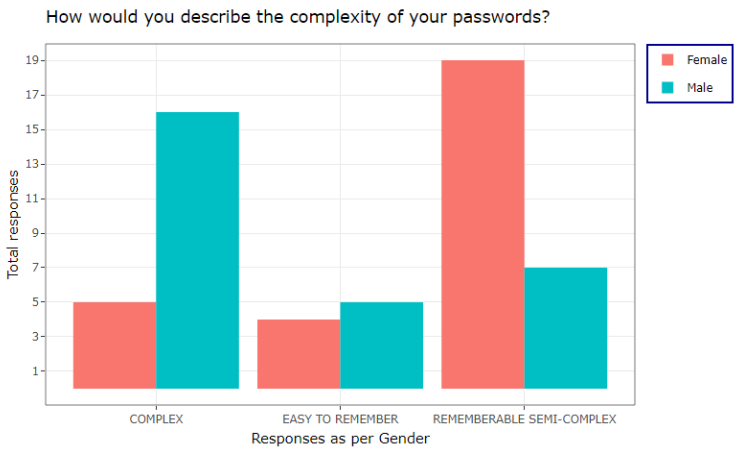

Figure 4.5: Password complexity per gender group

In terms of password complexity (*Q8), 21 respondents (37.5%) stated that they make use of complex password while 26 (46.4%) stated semi-complex passwords and 9 (16.1%) make use of passwords that are easy rememberable, as seen in Figure 4.5. For participants who stated that they make use of complex passwords, 71,4% were males. As for participants who stated that they make use of semi-complex passwords, the inverse trend is visible with 73% being female participants. Out of all participants, 31 (56,4%) make use of known or repeatable passwords for accounts as it is easy to remember (*Q9), while only 24 (43,6%) make use of a new password for each account. There is no significant difference in the gender distribution for those who use repeatable passwords and those who make use of new passwords. A survey employed by Google in 2019 found that globally, 65% of people reuse the same password for almost all accounts (Greene, 2019).

The *Protection of devices* subsection serves as an indicator of attitude respondents show towards the protection of devices in terms of the usage of anti-virus software and the back-up of data. When respondents were asked whether they use anti-virus software on their electronic devices (*Q10), 27 (48,2%) indicated that they use anti-virus software on all their devices, while 25 (44,6%) indicated they only use it on some of their devices and four (7.1%) who do not make use of anti-virus software. With regards to the gender distribution as seen in Figure 4.7, although the difference is not significant, more male respondents use anti-virus software on all devices while more female respondents use anti-virus software on some electronic devices.

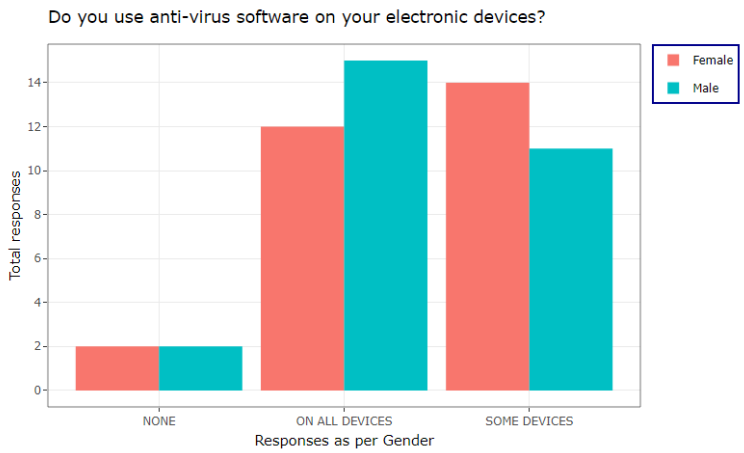

Figure 4.6: Anti-virus usage per age group

Most respondents (70,9%) indicated that they make use of anti-virus software that updates the application automatically (*Q11). For the minority of respondents seven (12,7%) indicated that they update their anti-virus software weekly, only two (3,6%) updates monthly and seven (12,7%) never update their anti-virus software. No significant difference is visible within the gender distribution for the frequency of anti-virus software updates. With regards to the back-up of data (*Q12), 27 (48,2%) stated that they regularly back-up their data, 25 (44,6%) stated that they only sometimes back-up their data and four (7.1%) stated that they never back-up their data. As seen in Figure 4.7 with the usage of anti-virus software, when referring to the back-up of data, the same trend is visible in the gender distribution. Figure 4.7 shows more male respondents regularly backing up their data while more female respondents only sometimes back-up their data.

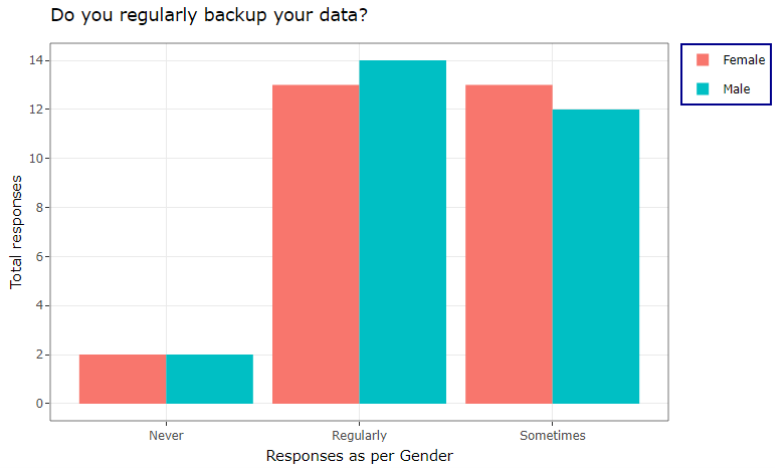

Figure 4.7: Data backup regularity per gender group

The purpose of the *Overall technology proficiency and awareness* subsection is to formulate a general idea of the overall security posture portrayed by participants with regards to the normal and daily usage of technology. More specifically, this includes the usage of Emails, making online purchases, doing the necessary background reading when signing up for something online such as newsletters, or simply how cautious or vigilant respondents are when handling technological devices.

When respondents were asked how vigilant and cautious they are when working with technology (*Q13), 42 (75%) respondents indicated that they always check to see that what they are doing is safe. 8 (14,3%) respondents do not find it a necessity to check if their interaction is safe and 6 (10,7%) of respondents do not know how to check whether their interaction with technology is safe. The gender distribution does not show significant difference in responses.

To investigate respondents' vigilance and caution further, they were asked whether they ever leave their PC or mobile devices unattended at their workplace (*Q16). 22 (39,3%) indicated that they never leave their electronic devices unattended while 29 (51.8%) indicated they only sometimes leave their devices unattended. Surprisingly, although in the minority, 5 (8,9%) respondents indicated that they regularly leave their devices unattended. A slight difference in the gender distribution can be identified in Figure 4.8. With regards to respondents who indicated that they never leave their devices unattended, the majority were male respondents, whereas more females indicated they only sometimes leave their devices unattended.

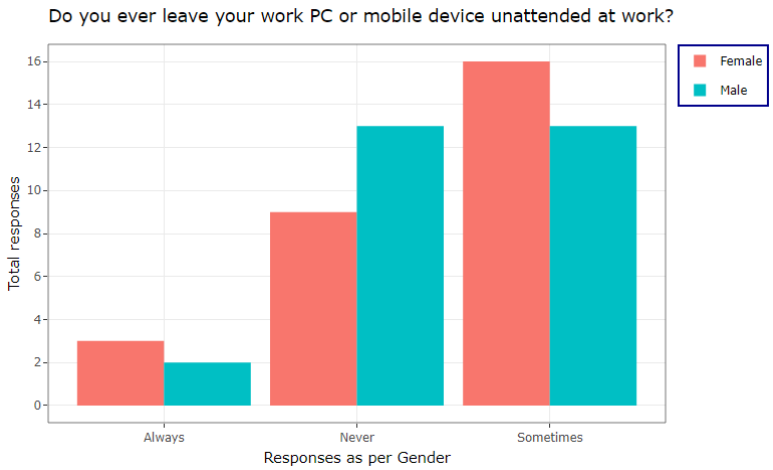

Figure 4.8: PC unattendance per gender group

With regards to the usage of Emails, the majority (57,1%) of respondents do not use their work Email address for any personal purposes such as subscribing to newsletters (*Q15). 19 (33,9%) respondents indicated that they sometimes use their work email address for personal purposes, while 5 (8,9%) use their Email address all the time. The gender distribution shows a slight difference in responses as seen in Figure 4.9. More female respondents indicated that they never use their work Email for personal purposes, while more male respondents indicated that they sometimes use their work Email for personal purposes.

Figure 4.9: Email usage frequency per gender group

Out of the pool of respondents, 26 (46,4%) indicated that they have never accidentally sent an Email to the wrong recipient (*Q18). 29 (51.8) indicated that they sometimes send Emails to the wrong recipient. Only one (1.8%) respondent makes this mistake frequently. Although the gender distribution show no significant difference in responses (Figure 4.10), more female respondents have never sent an Email to the wrong recipient, while more male respondents sometimes make this mistake.

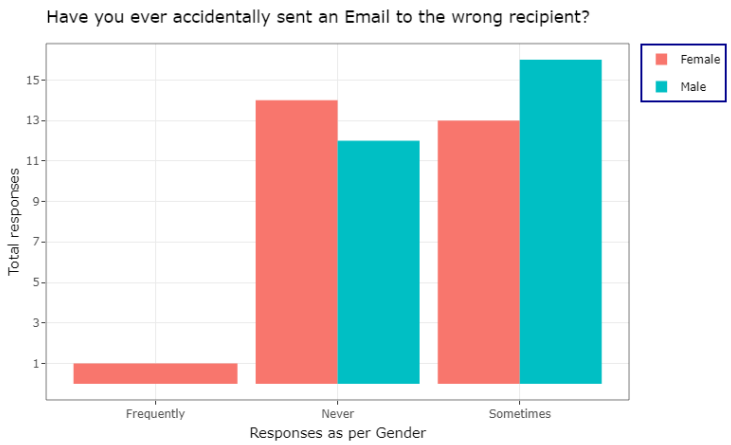

Figure 4.10: Emails sent to wrong recipients frequency per gender group

Similar to the question asking respondents regarding their Email usage, respondents were asked whether they ever use their company/work devices for anything other than work related activities (*Q14). 33 (58,9%) respondents indicate that they sometimes use their work devices for non-work-related activities. 12 (21,4%) respondents never use their work devices for non-work-related activities and 11 (19,6%) respondents always use their work devices for non-work-purposes. As can be seen in Figure 4.11, from those who indicated "Always" and "Never" the majority were male respondents, whereas those who answered "Sometimes", the majority were female respondents.

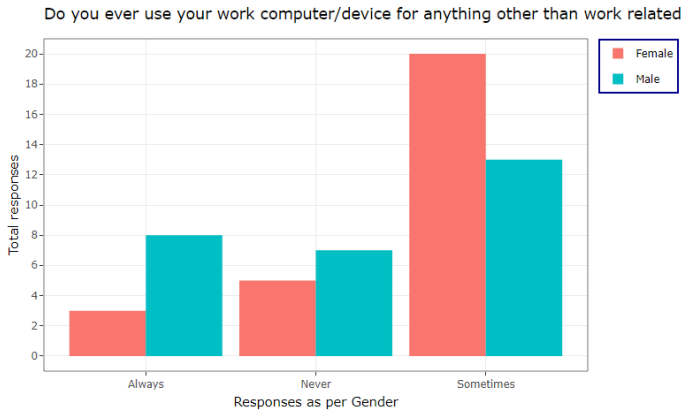

Figure 4.11: Work computer non-work related usage per gender group

When respondents were asked if they ever click "I Accept" without properly reading the terms and conditions when signing up for something online (*Q17), 30 (55,6%) respondents selected the "Sometimes" answer. 20 (37%) respondents selected the "Always" answer indicating that they never read any terms and conditions of subscriptions. Only four (7,4%) respondents indicated that they always read terms and conditions from selecting the "Always" answer. The gender distribution for each answer can be seen in Figure 4.12. More male respondents selected "Always" and "Never", while the majority of female participants selected "Sometimes".

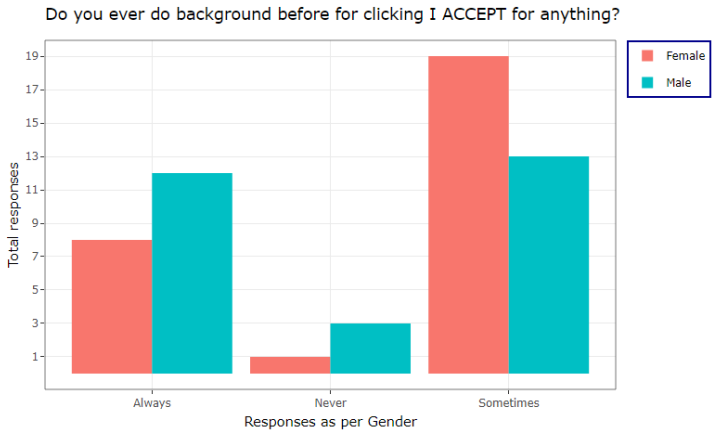

Figure 4.12: Gender group ignoring terms and condition messages

The last question for this subsection asked employees whether they make use of EFTs for online payments and if so, they should select their method of payment (*Q19). Only 10 (18,2%) respondents indicated that they do not make use of EFTs for payments. 28 (50,9%) respondents make EFTs directly on the website from where they want to make a purchase and 17 (30,9%) make EFTs to the receiver of the payment directly from their banking application. There is no significant difference in gender distribution with regards to the usage of EFT payments for participants. The use of EFTs from third-party websites was found to be extremely risky (Business Insider SA, 2020).

4.2.3 Risk identification and assessment

To investigate the potential threats that may arise from the risky, day-to-day activities that individuals may encounter in the modern digitised world of today, respondents were prompted with a series of open-ended questions. Open-ended questions were chosen as method for data capture as it allows respondents to provide uninfluenced unique answers. The goal of these open-ended questions (Survey Section B) was to capture respondents' individual and personal behaviours and responses when exposed to certain stimuli. In this case cyber threats within the digitised environment represent the stimuli. Stimuli-response questions were formulated and used as it is an effective way to understand and investigate behaviour as seen and stated by the Behavioral Learning Theory (Western Governers University, 2020). Both questions regarding respondents onsite and offsite usage of technology were used, from Survey Sections B1 and B2.

For the analysis of this section, a risk identification and assessment will be discussed for each section and its underlying responses. Thereafter, a table will be provided that summarise the risk identification, assessment, classification, and response. After a risk is successfully identified and assessed, Bojanc & Jerman-Blažič (2013) describes four options an organisation can respond to minimize the identified risk. These options include risk reduction, avoidance, transfer, and acceptance. The reduction of a risk is done by implementing appropriate technologies and policies that reduces potential loss and incident probability. Risk transfer entails transferring the risk to security or insurance agencies. Risk avoidance is done by eliminating the source of the risk in case where the risk severity is very high. Lastly, risk acceptance involves accepting that the risk will likely occur. Therefore, there is accommodated for the risk within business operations, for example by allowing a contingency fund to cover the cost that the risk may carry.

The following statistics obtained by (Sophos, 2020) provide background on the security posture of organisations in South Africa. The sample consists of 100 organisations that were surveyed in South Africa. The statistics provide insight on the risk assessment of the identified threats that will be discussed in the following subsections. Sophos provides the following statistics:

- The average fiscal impact caused by malware attacks for South African organisations are $266,817.18 (+- R3871 010.33). This includes operational and downtime cost because of the attack.
- South Africa has the fifth highest success rate in stopping ransomware attacks before it encrypts data (35% success rate). The global average success rate is 24,5%. Only Turkey, Spain, Italy, and Brazil have higher success rates than South Africa as seen in Figure 4.14.
- In 2020 only 24% of organisations in South Africa were hit by ransomware attacks.
- The two most targeted industries by ransomware attacks are “media, leisure and entertainment and “IT, technology and telecoms”.

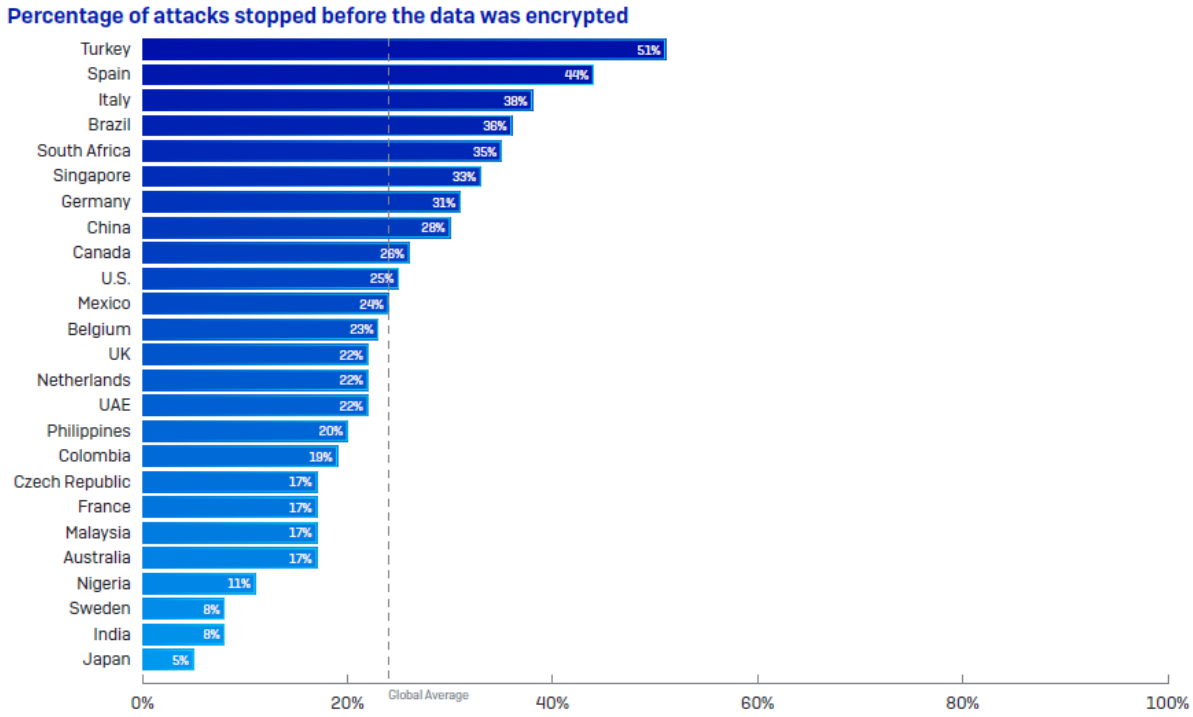

Figure 4.13: Percentage of attacks stopped before data encryption (Sophos, 2020)

Additionally, it is important to note that only as little as one single breach could be enough to make an organisation fold, regardless of the probability of occurrence. A breach can have a large fiscal impact, tarnish its reputation, and also result in operational downtime. It was found that 60% of business tend to fold after being the victim of an attack, 43% of attacks are aimed at small businesses while only 14% can defend against attacks (Steinberg, 2020). For the following survey questions analysis and risk measurements, because of limited available information, global average statistics will be used for the measurement of probability of occurrence. South African statistics, where available, will be used instead of global statistics. Table 4.1 will be used to rank the probability of an occurrence after being calculated in the following subsections.

Table 4.1 Risk probability intervals

Risk probability (P) [%]	**Probability score**	**Description**	**Probability of occurrence**
P <= 20	1	Rare	Highly unlikely, but can occur in exceptional circumstances
20 < P <= 40	2	Unlikely	Not expected, but low possibility that it can occur at some time
40 < P <= 60	3	Possible	The event can occur at some time as there is a history of casual occurrences.
60 < P <= 80	4	Likely	There is a strong possibility the event will occur as there is a history of frequent occurrences
80 < P <= 100	5	Almost certain	Very likely. The event is expected to occur in most circumstances as there is a history of regular occurrences

4.2.3.1 Survey Section B1

***Q1**: "How would you respond when you receive an Email from an unknown sender requesting personal information in your work Email inbox?"*

The majority of respondents show a high level of awareness of this occurrence as something that is potentially dangerous or malicious. The majority of responses include safe actions such as not responding to the Email or by blocking, ignoring, deleting or reporting it as spam.

> *"I would refuse or ignore the email as I do not give out sensitive information to unknown individuals"*
>
> *"Unknown sender is flagged and security is made aware if it looks malicious, otherwise deleted/ignored"*

However, in single cases (4/56), participants show interest in such Emails by either following up on the Email by conducting an investigation on the sender, the purpose and request of information.

> *"Check who is sender is, if I know the domain, and what they are asking for."*
>
> *"Verify validity before reading"*

By opening spam Emails, it holds the risk of potentially being infected by malware or containing links that lead to malicious websites. According to Chu (2021), by merely opening spam Emails is not significantly dangerous, but by opening attachments or links that pose the largest threats. Thus, the worst possible outcome for an organisation caused by an employee opening malicious spam Emails is that malware is downloaded and infects the organisations information system. Thereby malware gains access to sensitive data and information. The two most common types of malware that target, and infiltrate organisations are *Ransomware* and *Spyware* (Baker, 2021). According to (Sophos, 2020), the average cost for an organisation to remediate a ransomware attack for those who decline to pay the ransom is $732,520 USD and $1,448,458 USD for an organisation who carried out the ransom payment.

According to Cvetićanin (2021) more than 85% of Emails worldwide sent daily are classified as spam. Of all spam, Emails, phishing and fraud make up 2,5%. According to Richter (2020), one in every 412 (0,24%) Emails are considered as malicious.

As described in the literature review, the probability of an occurrence is determined by the nature of the threat, capability of the threat and the effectiveness and existing controls to defend against attacks. As only 24% of organisations in South Africa were hit by malware attacks in 2020 (Sophos, 2020), for the purposes of this study, this probability will be regarded as the capability of the threat to attack organisations in South Africa. As South African organisations hold a success of only 35% of stopping an attack before it causes damage, it will be regarded as the current effective of existing controls in South African organisations. Thus, 65% will be used as the variable for the probability that a malware attack will be successful on a South African organisation. These two variables will remain constant as the capability and existing controls variables for all the following calculations in this section. Additionally, the changing variable – the nature of the threat will change according to the specific type of threat identified for each question. For this question, the nature of the threat is malware that is distributed through usage and medium of Email, thus using 45% as its probability. With the use of these three discussed variables and actual South African malware statistics provided by Sophos, (2020), the following calculation is made:

Capability of the threat: **24%**
Nature of the threat: **45%**
Current effectiveness of existing controls: **65%**
Thus, $0{,}45 \times (0{,}24 \times 0{,}65) =$ **7,02%** probability of occurrence (7,02 < 20, thus get a P rank of 1)

The (0,24 * 0,65) part of the calculation will be recurringly visible throughout all the following probability calculations. Although the calculation depicts a significantly low probability of occurrence, such an occurrence can have a severe impact as described above. This severe impact is as a result of the potential loss of information integrity, availability and confidentiality (GOVERNANCE & STANDARDS DIVISION, 2017). It only takes one successful malicious Email attempt to make an organisation suffer and face the repercussions. The probability of 7,02% falls within the first probability interval 0 < P <= 20 as seen Table 4.1, thus receiving the probability score of 1. After considering the severity of ransomware attacks and the average

global and South African financial impact from such attacks, the risk impact receives a score of 5, giving it a total risk score of 5 and a classification of "Very Low". As mentioned in the literate review, organisations are just as secure as their weakest link, thus providing support for the above and following risk measurements.

***Q2**: "How would you respond when you are about to visit a website on your company device and the browser warns you that the website is unsafe?"*

The majority of respondents (37/56) will not continue with this action by either leaving the website, closing the browser completely or finding some other workaround without compromising any data. However, many respondents (19/56) still show indication of continuing to browse the site regardless of the warning message. Answers include a variation of actions such as by continuing anyway, finding a bypass to the site or browse the site with their own discretion. Examples of such responses are:

> *"Determine if the website is safe and assess the risks of going forward on the work device"*
>
> *"If it is a known site, ignore the message"*
>
> *"It depends. I might listen to recommendation or continue navigating in case now website well"*
>
> *"I would continue. I expect the company to make provision that would protect them from malicious websites."*

The majority of respondents who show indication of continuing to browse the site show a high level of confidence in the trustworthiness of the site as they believe that they are familiar with the site or have visited it before. Participants show that they are unknowing of the possibility that sites fake sites can pose as sights that they have visited before. By browsing unsafe websites, it can lead to various negative outcomes that impact an organisations. These outcomes include accidentally clicking on and downloading malware from malicious sites or the site atomically downloads the malware. This is also known as "drive-by downloads". Malicious software can also gather personal information and data stored on the machine that browses the site, even logging every key that you press on your keyboard (keylogging) and thereby aiming to capture usernames and passwords.

Visiting unsafe websites has the same potential worst outcome as opening spam Emails that are malicious – malware is downloaded and infiltrates organisations information and data. Hackers make use of exploit kits do automatically download and install malware as a person browses the web (Sectigo, 2020). According to Statista (2020), malicious web pages and web-ads account for 14% of malware infections globally as of 2020. A malicious website can either be infected with malware or used as a phishing tool (TESSIAN, 2020a). According to Google's Safe Browsing Report (Google, 2021), between 2007 and 2019, there has been a significant increase in the number of phishing websites detected, whereas malware website detection shows a significant decrease as seen in Figure 4.14.

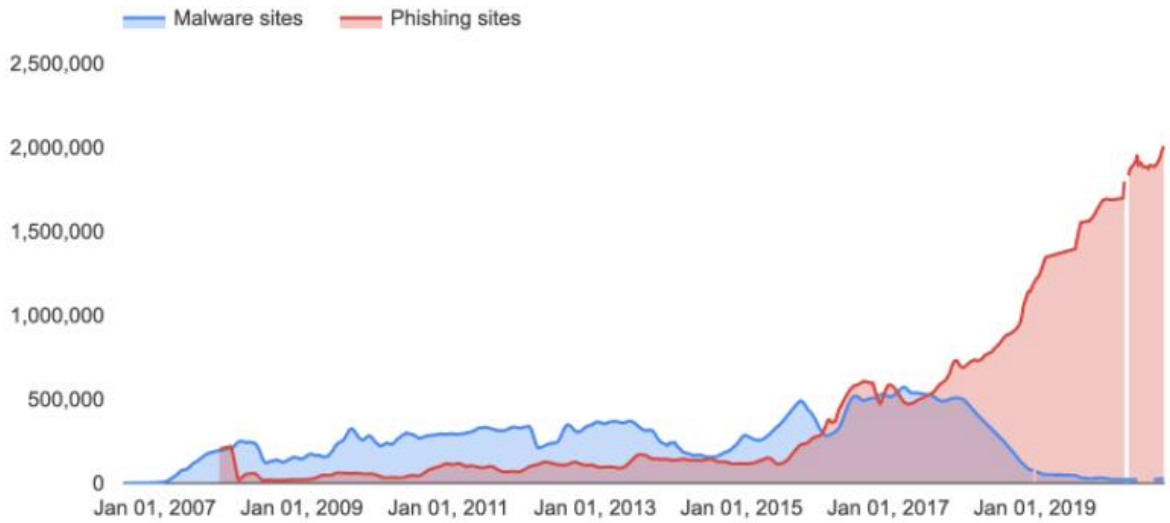

Figure 4.14: Global malware vs phishing sites between 2007 - 2019 (TESSIAN, 2020a)

The probability that a South African organisation will be used hit by malware originated from a browsed, is 2,2% ($0{,}14 \times 0{,}35 \times 0{,}65$). This is as a result of 14% of malware globally that distributed through websites, as mentioned above and the constant capability and control variables of 24% and 65%. This threat receives a probability risk score of 1.

***Q3**: How would you respond when your workstation prompts you to do a system update or any other update?*

Most respondents will proceed with the updates although there are a few exceptions as to when the action will be carried out. Many participants stated that they will postpone the update to a more suitable time such as after hours. Others will seek confirmation from management before proceeding with the update and a few completely ignore the update. The high majority of

participants (52/56) are in favour of doing system updates, although some being scheduled for a more suitable time. Only 4/56 (7,143%) did not deliberately state that they will do the update and will either ignore it or delay the update for as a long as possible. By delaying system updates, it leaves potential holes, flaws or weaknesses in software and thereby potentially leaving a back door for attackers to infiltrate. Although ignoring an update may not pose a risk or necessarily be crucial in every circumstance, the potential worst outcome may be of that leaving a weak point that could be exploited.

According to (Boblin, 2018), the top reasons why people neglect or ignore computer updates are as a result of compatibility issues with updates software. Additionally, they are uninformed about the importance of updates, people are comfortable with the software as it is before the update or that a person may have bad experience from a previous update. All these factors are personal to an individual, yet the potential threat from not updating software remains. An example of a massive global cyber-attack known as "WannaCry" infected more than 300 000 computers in 2017 (Fruhlinger, 2018). For individual people, this attack could have been prevented if only they had updated their computer software (Redmiles, 2017). According to Scientific American (Redmiles, 2017), only 64% of security professional update their software regularly or immediately upon release, while only 38% of regular users take the same action. Additionally, Scientific American states people with computer expertise tend to update software faster, with an average of 24 days passing before software is update in comparison with regular users who have an average of 45 days before the same updated is completed. They assume that this difference in behaviour might be as a result of experts being more aware and informed about the vulnerabilities that may be fixed from the update.

For the threat identified from not updating software, 72% of users do not take immediate action when updates are available, thus being the nature of the threat. Similar to worst outcomes described in Q1 and 2, by not updating software it may lead to the infiltration of malware and large financial damages. The following calculation determines the probability that non updated software may lead to a data and security breach – $0{,}72 \times (0{,}24 \times 0{,}65) = 11{,}2\%$. This probability risk score receives a rank of 1.

***Q4**: "How would you respond when your workstation warn you that a virus has been detected on your computer?"*

The majority of respondents show a high alert response and will take immediate action by either reporting the situation to IT/management within their organisation or take self-action such as running an antivirus scan and removing the virus accordingly. Only 5/56 (8,93%) respondents show no indication of taking appropriate action or do not believe that such an occurrence will not happen to them. However, some participants show a high level of awareness and preparedness for such an occurrence. Additionally, they state that they will disconnect or isolate the device before further investigation. Examples of such responses:

> *"Isolate the device via our anti-virus cloud management console and investigate the device in safe mode, if the anti-virus has not deleted/contained the malware"*

> *"Disconnect network and investigate source, then research infection name on another device"*

> *"I would not open any documents or apps and I would investigate the possible point where the virus was introduced to my computer (e. g. vis spam email)."*

According to Chron (Kazmeyer, n.d.), the three main consequences of not having adequate and up-to-date security software are the loss of data, the loss of time and financial costs. They elaborate that cleaning up and recovering from virus attacks are very time consuming and can even cause employees to be unable to perform their work for a period of time. This is due to the infected devices being shut down in order to deal with the viruses. Additionally, not only is adequate anti-virus software expensive, but the cleaning and recovery process can become very expensive as well. As of 2019, cyberattacks and incidents in general cost businesses $200 000 on average whereas, 43% of online attacks are aimed at small organisations with only 14% with prepared defense strategies in place (Steinberg, 2019). CNBC (Steinberg, 2019)highlight the fact that all modern organisations will eventually face a security breach, again supporting the importance of preventing even the smallest chance of a security breach. According to AfricaCenter (Allen, 2021), 96% of security breaches stay unreported and unresolved in African countries. Accenture (Mcanyana et al., 2020) supports this statement with the focus on South Africa with reasons as to why South Africa is such a popular country for cybercrimes. The main reasons are that insufficient funds cause a lack of investment in cybersecurity, South Africans have poor knowledge on cyber threats and risks. Additionally, it was stated that South

Africa is especially slow at adopting cybercrime legislation. According to CSO (Grimes, 2020) viruses make up less than 10% of all malwares. For the probability that computer will be infected by a virus, the calculation is as follows – $0{,}1 \times (0{,}24 \times 0{,}65) = 1{,}6\%$. This threat receives a probability risk score of 1.

***Q5**: "How would you respond when you suddenly experience the company Wi-Fi to be slow and you need a better data connection in order to complete an important task on time?"*

For this particular question, respondents provided mixed reactions and answers. The answers are divided between actions such as respondents using their own mobile data (personal hotspot) and simply continue working. Furthermore, respondents reporting the problem to management, respondents self-investigate the problem such as the cause of the slow connection or by restarting the router or connection. Although the usage of personal devices is assumed to be less secure, notably a few respondents stated that they are allowed to make use of their own data supply or have been supplied with a wireless device from the organisation.

> *"Use my company supplied APN connected cellular device"*
>
> *"Our company also gave us Vodacom wireless routers for cases like this"*

Single respondents make use of private connections, but through a secure connection such as VPN. Some respondents have alternate company provided networks that they can switch to.

> *"I would connect to a different VPN (we have several) or I will work from home and connect to that wifi"*
>
> *"Use my private wifi through my private VPN service."*

One participant explicitly stated that they will make use of a public Wi-Fi network in order to continue with their work. The possible downsides to using one's own personal data connection or making use of a public network is that a respondent's personal device can be unknowingly infected with malware. This can cause a weak point for an attacker to gather access credentials to the organisation. With the usage of mobile or personal devices in the workplace, an incident or breach may not even be detected by the organisation's incident response team. With the usage of public Wi-Fi networks to connect to company portals, if the connection is not secure, an attacker can intercept data transfers between the respondent's device and the organisation.

Thereby, data can get stolen, or access can be gained to the organsisation. This type of attack is also known as a "Man in the middle attack" (Swinhoe, 2019). According to Securelist (Legezo, 2016), roughly 24,7% of public Wi-Fi hotspots do not use encryption to secure its connection. The worst potential outcome for this scenario is also that of malware being installed or distribution to the organisation's sensitive data and information. According to (Check Point, 2021), globally, roughly 40% of mobile devices are vulnerable to cyber-attacks. By only bringing the usage of personal mobile data into account, the probability that a personal device will fall victim to a cyber-attack and thereby cause a threat to an organisation in South Africa is – $0{,}4 \times (0{,}24 \times 0{,}65) = 6{,}2\%$. By only bringing the usage of public Wi-Fi networks into account, the probability percentage is – $0{,}247 \times (0{,}24 \times 0{,}65) = 3{,}9\%$. This threat receives a probability risk score of 1.

***Q6**: "How would you respond when working on your work computer and an advertisement pops up relating to something or product you recently browsed?"*

Most respondents (52/56) stated that they will not investigate pop-up advertisements, shortly known as "Ads" by either completely ignore the advertisemennt or by blocking and removing it.

> *"I close it as quick as I can, without even attempting to read the ad."*
>
> *"I would most likely briefly check out the advert should it be safe to do so"*
>
> *"I don' browser anything not related to the work and if does happen the advert will be blocked it its find to malicous"*

Many respondents show a high level of irritation from the presence of ads, while only four respondents explicitly stated that they will investigate an ad once it appears. Although most advertisements only aim to sell you a product or try get your contact information (non-malicious intent), advertisements with malicious intent yet exist. According to (SPAM LAWS, n.d.) these types of advertisements, also known as *Malvertising* (Norton, n.d.) aim to forcefully take your information by once clicked on. This will initiate a download and install viruses such as *Trojan Horses* on your computer which can then open the door for various other malware to be distributed. People fall victim to Malvertising by either clicking on an infected ad or by visiting the website that is home to the infected ad. This malware distribution process is also known as "Drive by downloads" and can infect a computer as fast as once the ad is successfully

loaded (Norton, n.d.). What makes this type of malware distribution more prevalent and successful is due to attackers' strategy to buy legitimate space on advertisement networks and in return hope to get the ad to be run by legitimate websites. Thereby, with the advertisement being associated with a legitimate website, it decreases the level of suspicion from a person browsing and increases the chances of being clicked on. Fraudulent and invalid ads consist of 36% of all clicked ads (PPC Protect, 2021). The probability that a fraudulent or dangerous ad that will be clicked on may impact an organisation is – $0{,}36 \times (0{,}24 \times 0{,}65)$ = 5,7%. This threat receives a probability risk score of 1.

***Q7**: "How would you respond when your current device is connected to company Wi-Fi and a social media notification pops up?"*

Most responses (39/56) steer towards not opening the social media notification. This is done mostly by ignoring the notification, blocking/disable notifications, not connecting personal devices to company Wi-Fi at all or by not using company provided data for personal use. Most of the participants who showed interest in such notifications (17/56) stated that they will check the popup right away or at an appropriate time such as during breaks or lunch. Not only can social media be a distraction or a waste of time for employees at work, it can also be a tool for exploitation and distribution of malware for people with malicious intent (PandaSecurity, 2021). As social media platforms are a highly popular network for the distribution of videos, images and links, attackers also seek to exploit this platform to distribute their malware and infiltrate or steal information. An attacker will usually disguise them as someone you know, perhaps a close friend or even family members and thereby fool you with their familiar appearance to click on an image or a link. According to Lazic (2021) 83 million accounts (5%) that exist on Facebook is fake and one in every 10 profiles on a free dating site is fake. As of 2020, 28% of frauds that were reported globally were initiated on social media platforms (Data Spotlight, 2020). According to the statistics provided above, the probability that a fraudulent and fake social media account will steal organisational related information from a person in South Africa is - $(0{,}28 \times 0{,}05) \times (0{,}24 \times 0{,}65)$ = 0,2%. This type of threat has an extremely low probability.

***Q8**: "How would you respond when prompted by a colleague (well known or not) to share access credentials for any particular reason?"*

Most respondents (46/56) will refrain from providing any personal credentials. Only a few respondents (10/56) show willingness to provide credentials and will do so depending on the nature or reason of the request or by changing the credentials afterwards. Single participants will only do so once approved by authority or management. Although this action might be approved by management, the risk still remains that lender of credentials can cause a weakpoint or mistake. A weakpoint or mistake can lead to an exploitation. According to Outpost st. Clair (n.d.), there are numerous risks involved from the sharing of account passwords. This includes comprise of several other accounts which use the same credentials, the lender of your credentials accidentally leaks your information to people with malicious intent or they misuse the privileges assigned to your account.

According to Kratikal (Dutta, 2020) 42% of employees share their work account credentials for collaboration purposes and that less than 20% of employees are aware of the organisation's credential sharing policy. As previously mentioned, it only takes one incident for a large data breach to occur, such as in this case, a singular employee who shares or reuses passwords for a breach to occur. Kratikal (Dutta, 2020) mentioned an occurrence where 60 million customer credentials were stolen from a data breach which resulted from a single employee who reused passwords. The probability that the sharing of account credentials may lead a security breach is thus calculated as follows – $0{,}42 \times (0{,}24 \times 0{,}65) = 6{,}6\%$. This threat receives a probability risk score of 1.

4.2.3.2 Survey Section B2

Q1*: "How would you respond when you receive a phone call requesting personal information of either you or your organisation claiming to be from your company or someone you know?"*

None of the respondents from the pool of participants will provide the requested information without hesitation. Most respondents state that they will immediately end the call, block it or report the call to management. It is visible that there exists an uneasiness among respondents when prompted to reveal personal information over a phone call.

> *"I feel a bit uneasy and at the same time will try and find a way to get the data and information in a more systematic process and me comfortable and makes the information more safe and secure"*
>
> *"Tell them that I am not comfortable answering"*

> *"I won't provide that. It's personal"*

However, although hesitant at first, many participants will further investigate the legitimacy of the request and raise concerns with HR or management.

> *"I would refer the person requesting the information to either my manager or HR. "*
>
> *"Hang up. If claiming to be from my company then raise it with management."*
>
> *"i normally say please send me an email, i would not give any info out without making sure it is valid"*

Although from the pool of participants there is a reluctance visible for giving out personal information, threat and possibility of occurrence yet remains. According to SCAMWATCH (2021), as seen in Figure 4.15, scam phone calls are the highest among all the various delivery methods recording thus far in 2021.

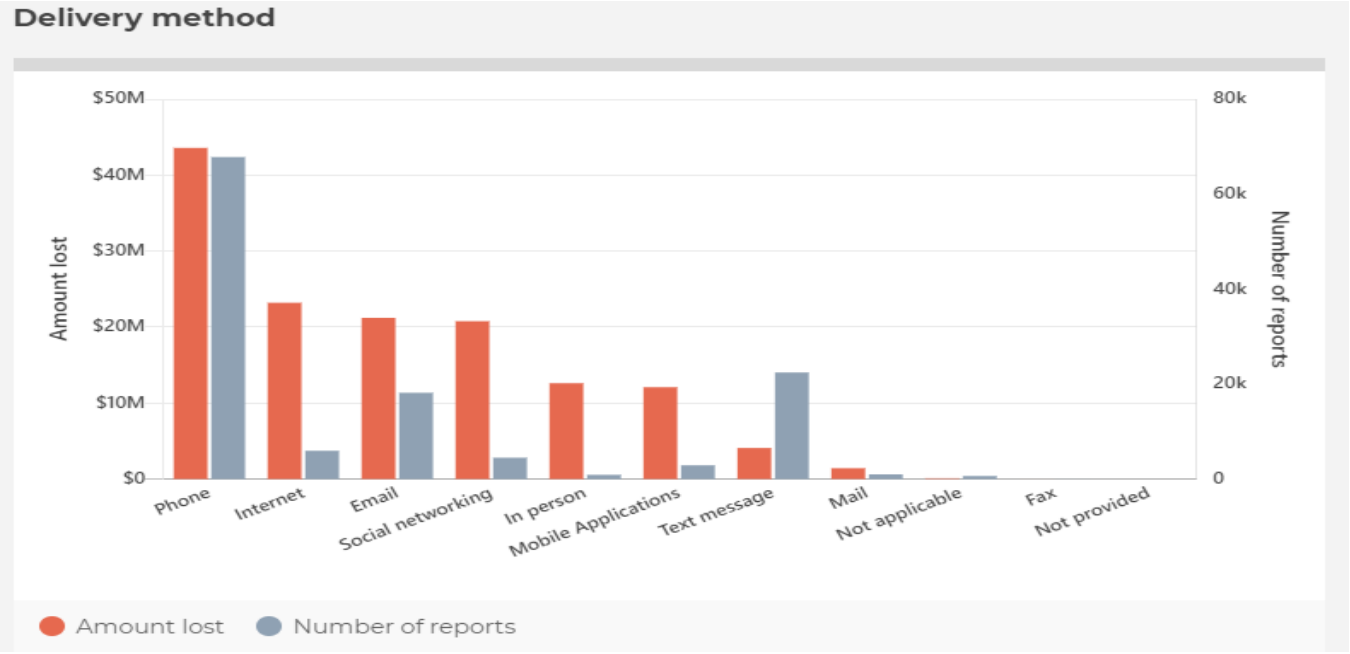

Figure 4.15: Global scam delivery methods (SCAMWATCH, 2021)

According to ageUK (2021), most phone scams are banking related scams, computer repair scams, compensation calls relating to an occurrence of an accident. In addition, this includes tax and insurance claim scams and pension and investment scams. As it is evident that phone

related scams are by far the most popular method used by scammers, the assumption is made that any person owning a mobile phone should be cautious and can expect the inevitability of encountering a scam phone call. According to ZdNet (Brown, 2020) more than half 54% of all phone calls are spam calls and 22,6% of people would answer their phone to an unknown caller. By using global statistics, 58% of all spam calls are fraudulent of nature (Cook, 2021). According to the statistics provided above, the probability that a person will encounter a fraudulent phone call and in the worst case, reveal sensitive information that could lead to financial damages for an organisation in South Africa, the calculation is as follows. 54% (percentage of calls that are spam) * 58% (percentage of spam calls that are fraudulent) * (0,24 * 0,65) = 5%. This threat receives a risk probability score of 1. Additionally, as seen in figure 4.16, text messages hold the second highest number of reports. This is as a result of "Smishing". Smishing works similar to any other method of phishing, but in this case, the medium is via a nefarious text message (Kaspersky, n.d.).

***Q2**: "How would you respond when you need to connect to your organisation's information system, but you are at an offsite location?"*

The majority of respondents acknowledged the need to use a safe connection when in need to work or connect from an offsite location, thus stating the use of a company provided or personal VPN in order to secure the connection.

> *"Use the company VPN to connect to the systems."*
>
> *"I would connect remotely using secured company resources."*
>
> *"I use my secure LTE provided by company."*

Some respondents stated that in the case of such an occurrence they will request assistance from IT or management.

> *"Our company has an allocated IT assistance number especially for this."*
>
> *"Call IT help desk for assistance"*

Only 12 respondents (21,43%) stated that they will connect to their company's information system with their own personal data connection. They state this without the mention of a secure

procedure to secure the connection such as with the use of a VPN. Similarly, to the risks as identified in Section B1 Question 5 from using one's own personal data connection or public Wi-Fi networks, the threat of data interception and infiltration yet remains and thus the same probability calculation is used. For mobile phone vulnerability to an attack $= 0{,}4 \times (0{,}24 \times 0{,}65)$ = 6,2%. For the risk probability of connecting a device to a public Wi-Fi network – $0{,}247 \times (0{,}24 \times 0{,}65)$ = 3,9%.

***Q3**: "How would you respond when you receive random friend requests on social media from persons claiming to be your friend or someone you know?"*

The majority of respondents will either decline, ignore or block such requests on social media. Those respondents who stated that they will accept the request will only do so when believed or perceived that they know the person. It is not visible from respondents' answers that they consider the possibility that the request could be someone who is impersonating a friend, family member or a colleague.

> "Random: I would ignore it, a friend I know, I might accept depending on the person"

> "If I do know the person or see that we have a lot of friends in common, I may consider accepting the invite"

> "Only accept that request if it is someone I actually know and want to be friends with on social media"

Only two respondents stated that they will accept the request without mentioning that they will investigate its legitimacy.

Similarly, to the risks and threats identified at Section B1 Question 7, this question focuses more specifically on the reactions to random social media friend requests and the potential risks associated with that action. As previously discussed, attackers use social media platforms to disguise their appearance as someone familiar in order to fool a user by accepting their request and clicking on malicious content. According to CMIT Solutions (2021) through social media hackers use social engineering techniques to spam a personal email address. This email address is accessed as a result of it being visible to the connection on a social media account. In addition, hackers attempt to discover the identity of your close friends, colleagues as well as

bosses in order mimic a user that may seem legitimate to you. Thereby, hackers hope that financial requests will be processed by an uninformed or naïve employee. As discussed in Section B1 question 7, the probability fake "friend" will contact you on social media with malicious fraudulent intent is - $(0{,}28 \times 0{,}05) \times (0{,}24 \times 0{,}65) = 0{,}2\%$.

***Q4**: "How would you respond when you need an internet connection on your company device at an offsite location and public Wi-Fi networks are available?"*

For this specific question, the focus is on the overall need for internet access on a company device and not to connect to the company information system/portal. Surprisingly, in this particular case, the majority of respondents stated that they will make use of the public Wi-Fi (46/56). 18 (32,1%) respondents stated that they will make use of the public Wi-Fi connection without discretion and without mentioning any method of securing the connection. 9 (16,1%) respondents stated that they will make use of the public network connection, but with the exception of using a VPN to secure the connection. 13 respondents (23,2%), with and without the use of a VPN, will rather make use of their own connection than using a public Wi-Fi network. Only 10 (17,9%) respondents stated that they will never use public Wi-Fi networks. From these 10 respondents, some do not give an indication of what they will do instead of connection to the public network. The remainder would rather contact management on how to approach the situation with an appropriate solution. Two respondents stated that they have a company provided device which provides a data connection when at an offsite location. Although the motive of this question differs from Section B1 question 5 and Section B2 question 2, the risk probability and threats are identical. For mobile phone vulnerability to an attack = $0{,}4 \times (0{,}24 \times 0{,}65) = 6{,}2\%$. For the risk probability of connecting a device to a public Wi-Fi network – $0{,}247 * (0{,}24 * 0{,}65) = 3{,}9\%$.

***Q5**: "How would you respond when you realise you have sent an Email to the wrong person that contains classified/personal business information?"*

Most respondents stated that they will take immediate action by trying to recall/retract the Email. In addition to trying to rectify the mistake, many participants will consult or report the incident to authority or management.

> *"I would retract the email if possible or contact IT Administrator for assistance."*

> *"Report to my manager and let the recipient know to please ignore and delete the email"*

Many respondents will also contact the receiver to try and rectify the mistake from their side.

> *"I would try and recall the email, failing which, I would try and contact them directly and explain the error and consequences"*

> *"Make every effort to either recall or to get the recipient to delete the email."*

Among the pool of participants, a high sense of responsibility is evident that they take the matter seriously and act accordingly to try and rectify the mistake as soon as possible.

According to Tessian research (TESSIAN, 2021), 58% of employees admit that they have at least once sent an email to the wrong recipient. It was also stated that a case such as sending an Email with sensitive organisational or customer related information to an irrelevant recipient should be treated as data loss incident and security breach. This incident or breach can have severe consequences for both the employee and the organisation (TESSIAN, 2020). Taking the research mentioned into account, the probability that an Email that is sent from an employee to the wrong recipient potentially leading to a data and security breach, the calculation is as follows. $0{,}58 \times (0{,}24 \times 0{,}65) = 9{,}04\ \%$. This threat receives a risk probability score of 1.

4.2.3.2 Subsection Conclusion

As described by GOVERNANCE & STANDARDS DIVISION (2017) in the literature review, the potential loss of information integrity, availability and confidentiality are used to determine the impact of a threat on an information asset. According to UpGuard (Tungall, 2021), the value of information assets needs to be determined by the organisation before the impact of a threat on the asset can be assessed. Due to the nature of this study, with the focus being centric on human vulnerability and its resulting risks, as well as the design and aim of the methodology, organisation specific information is not available. Due to the limitation of the data collected only focusing on human behavioural aspects and perception, the impact measurement for the identified risks and threats in this section will be assessed based on general assumptions and web research. As discussed, the worst possible outcomes from a security breach caused by the threats identified from respondents' answers, are that of malware infiltrating and gaining access/control of the organisations information and data. Due to the versatile nature of cyber

criminals and their methods, similar outcomes can be achieved through various methods of exploitation or infiltration with the same intention. For e.g., cyber criminals can distribute malware through malicious websites, Emails, advertisements, unencrypted networks etc. As a result of the nature and capability of the malware, the risks identified by each survey question have received an impact score of five. An impact score of five represents the worst possible outcome in terms of repercussions and fiscal impact for an organisation. The different scales of impact and its description can be seen in figure 2.6 (Kure et al., (2018)). Table 4.1 and Table 4.2 summarises and displays the identified risks, its associated probability and impact scores as well as the appropriate response action.

Table 4.2: Risk assessment Survey Section B1

	Risk ID (Survey question Section B)	Identified Risk	Internal vs External	Risk probaility (1-5)	Risk probability perecentage %	Risk Impact (1-5)	Total Risk score /25	Risk Classification	Effect on organisation	Risk Response (Accept/Avoid/Mitigate /Transfer)	Response Strategy
SECTION B1	Q1	Open spam/malicious Email with malicious attach or link	External	1	7,02	5	5	Very Low	Stolen/Encrypted data. High financial costs	Accept	Educate employees on spam Email awareness and risks. Use spam blockers etc.
	Q2	Visit infected/malicious website containing malware	Internal	1	2,2	5	5	Very Low	Stolen/Encrypted data. High financial costs	Accept	Educate employees to identify potential unsafe websites. Implement stronger firewalls to completely block unsafe websites.
	Q3	Potential weakpoint in system stays unfixed/ backdoor	Internal	1	10,8	5	5	Very Low	Exploitable gateway for countless other viruses/threats. Buggy software. High financial costs	Accept	Implement auto-update features for sofware. Regular check-ups on non-updated software. Stricter rules for the rollout of future software updates.
	Q4	Ignorance of warnings and outdated anti-virus sofware can lead to distribution of malware	External	1	11,2	5	5	Very Low	Time and data loss. Device shutdown, high recovery costs	Accept	Hold employee acountable for irresponsible actions. Employ stricter rules on the update of anti-virus software/ immediate auto update of software.
	Q5	Using unsecure personal and public networks to connect to/access work systems	Internal	1	6,2	5	5	Very Low	Evesdropping on access credentials. Stolen/ data loss. High financial costs	Accept	Restrict access from offsite locations and dedicated devices.
	Q6	Respondent fall victim to "malvertising". Clicks on malicious link or image	External	1	5,7	5	5	Very Low	Stolen/Encrypted data. High financial costs. Disruption of business processes.	Accept	Educate employees to identify potential malicious advertisements. Implement stronger firewalls and usage of adblockers or work devices.
	Q7	Malicious links or image gets clicked on on Social Media pages	External	1	0,2	5	5	Very Low	Loss of data and money due to fradulant transaction. Unauthorised access to organisational data. Leakage of sensitive data	Accept	Restrict the use of social media on company networks and devices. Exceptions for social media usage that forms part of work-related activities. Education on threat awareness
	Q8	Shared credentials get leaked to person with malicious intent/ account gets locked	Internal	1	6,6	5	5	Very Low	Leakage of sensitive organisational and client data. Unauthorised access to organisational	Accept	Forbid the share of access credentials. Disciplinary actions agains violations.

Table 4.3: Risk assessment Survey Section B2

	Risk ID (Survey question Section B)	Identified Risk	Internal vs External	Risk probaility (1-5)	Risk probability perecentage %	Risk Impact (1-5)	Total Risk score /25	Risk Classification	Effect on organisation	Risk Response (Accept/Avoid/Mitigate/Transfer)	Response Strategy
SECTION B2	Q1	Sensitve information gets revealed to spammer/attacker	External	1	5	5	5	Very Low	Exposure of sensitive information. High financial damages and loss.	Accept	Provide education of the identification of spammers and necessary actions to be taken.
	Q2	Using unsecure personal and public networks to connect to/access work systems	Internal	1	6,2	5	5	Very Low	Evesdropping on access credentials. Stolen/ data loss. High financial costs	Accept	Restriction on personal device and public network access to information systems.
	Q3	Respondent fall victim to Social Media scammer and personal information about organisation is exposed and	External	1	0,2	5	5	Very Low	Loss of organisational money and data	Accept	Educate and raise awareness on the risk and identification of social media scamming.
	Q4	Using unsecure personal and public networks to connect to/access work systems	Internal	1	6,2	5	5	Very Low	Evesdropping on access credentials. Stolen/ data loss. High financial costs	Accept	Restriction on personal device and public network access to information systems.
	Q5	Classified/sensitive information exposed to a person with malicious intent	Internal	1	9,04	5	5	Very Low	Sensitive information and data exposure	Accept	Hold employee accountable for incident. Use Email that has revert options for messages.

4.2.4 Personal & organisational related perceptions (Survey Section C)

For this subsection of questions, similar as with Section B, open-ended questions were used. This enabled to gathering of personal information regarding respondents' perception on digital risks and threats. In addition, the perception of the security culture and requirements within their own organsisation was gathered. The results from this section as well as in combination with section A will aid in the estimation of the security posture already portrayed by the workforce. For the qualitative analysis of respondent's answers, the software tool, *Taguette* was chosen as the appropriate tool. *Taguette* is a free and open-source tool for qualitative research. One can import research findings, highlight and tag quotes, and export the results. This software was chosen as it is commonly known and used for studies that analyse qualitative data, as *Taguette* allows one to identify qualitative themes in the research findings. A full list of the open-ended questions for survey Section C can be seen in Appendix A.

4.2.4.1 The importance of data and information security (Q1)

With regards to respondents' perception of the importance of information and data security in organisations, most respondents immediately center their answer around the value and safeguarding of confidential information. This confidential information includes those of customers/clients as well as organisation specific data and information such as of employees' and intellectual property.

> "*Yes and I believe that it is the responsibility of the company to ensure that measures are in place to protect their data, employee data and client data.*"

> *"Yes I do. It is very important to main customer data security in order not to compromise any sensitive information"*

Many respondents refer to regulatory compliance acts such as GDPR and POPIA to enforce the importance of maintaining and handling client information and data security.

> *"Legally under POPIA or GDPR. Ethically, the responsibility to those to whom the data pertains."*

> *"Yes, because of POPIA"*

Many respondents confirm the importance of information and data security in organisations, but provide a generic reason for their answers or provide no motivation at all. Those who provided generic motivations for their answers acknowledge that personal information is valuable, and organisations are liable to secure personal information and data in order to avoid the inevitability of data breaches.

> *"Yes, pre-emptive security avoids the inevitable"*

Other respondents acknowledged the importance of information and data security by emphasising the potential consequences an organisation may face from not having ample security mechanisms. These consequences mostly relate to the exploitation of vulnerabilities by people with malicious intent where this may lead to legal action, fines, blackmailing or even bankruptcy.

> *"Yes, attackers will try to find any and all opportunities to exploit any vulnerabilities they find to either gain the upper hand against you, or to cripple your organization."*

> *"Yes, data breach is serious can lead to fines and legal action yes, it drives decision making"*

Overall, the majority of respondents show a high level of awareness regarding the importance of information and data security and an understanding of its significance and impact the lack thereof may have on organisations.

4.2.4.2 The understanding of the term "*Digital risks*" (Q2)

For those respondents who show an understanding of digital risks, the answers revolve around three main themes: Risks relating to cyber-attacks/threats/breaches, risks relating to data introduced to digital ("online") world and risks specifically introduced through the use of technology/devices. With regards to the risks relating to cyber attacks or breaches, respondents frequently describe digital risks as the vulnerability to be "hacked", or information to be "leaked" and essentially, data being exposed or end up in the wrong hands.

> "*Leaking, Hacking of data to persons other than the owner of the data*"

With regards to the risks relating to the presence of data in the digital world, respondents' correctly make the association between risks and threats "*that are posed to you by the digital world*". Words used to describe this association are "online", "connected", "digital" and "data". In a business sense, respondents also frequently refer to the risks that an organisation may face as a result of using a digitised or online platform to conduct business and data that is electronically accessible.

> "*Digital risks according to my understanding involves all risks involved when using digital mediums to conduct day to day tasks (business or social)*"

With regards to the risks introduced by the usage of technology, respondents refer to the vulnerability of technology in general that may lead to a breach and exposure of valuable information. Two respondents shift the focus to humans and associate digital risks to the extent where human behaviour and interaction with technology are the lead cause of vulnerability.

> "*The biggest risk is that of human error, then aspects such as device security, internet access security, institution firewall security etc.*"

Lastly, some participants (10/56) show a lack of surety and are completely unfamiliar with the term.

> *"not too sure, haven't heard of the term"*

> *"I am aware but could always learn more."*

4.2.4.3 The impact of work-related stress on technology proficiency (Q3)

Respondents' answers show a large variance in work-related stress levels, between high stress levels, low stress levels, varying stress levels and stress levels described by participants as "average/medium". Those who indicated varying stress levels state that deadlines/timelines and specific projects determine the stress level they experience at work. Some participants state that technology may be the cause of the stress they experience. The describe "slow network"

as the reason that impedes them from working effectively, rather than overall stress being the impediment of proficiency.

According to respondents' answers, a general trend emerges depicting that technology proficiency is not affected by experienced stress levels at work. This is seen in the majority of respondents who described their stress level and whether this level affects their stress or not.

> *"In general I am not stressed at work and I do not think that a heightened experience of stress would influence my proficiency with technology."*

> *"I have high stress levels, but since I work woth technology daily, I am so in tuned with it that it does not influence my proficiency with technology."*

However, in single cases, there are respondents who stated that stress does indeed affect their technology proficiency.

> *"Yes, high stress levels can lead to rushing things, which could lead to someone being sent the incorrect email for example."*

> *"Medium. yes, urgency causes oversight"*

Although it appears that the majority of respondents' technology proficiency is unaffected by work related stress, it is mentioned in the literature review that stress and burnout are one of the causes of error. This is applicable as once again it only takes one person to make a mistake that jeopardises the organsisation security.

4.2.4.4 Organisational security culture (Q4 - 9)

This subsection discussion contains all the questions directly involving respondents' organisation and their perceptions of certain aspects such the organisational security culture and the expectations the organisations have of their employees in terms of security behaviour.

With regards to the perceived security culture from respondents within their organisations (Q4), it is clearly visible that most organisations take information and data security very seriously. Respondents make use of words such as "serious", "pivotal", "important", "careful", "stringent", "strict" interchangeably when describing how the organisation regard information

and data security. Some respondents provide answers that appear that their organisation has a serious security culture, but do not explicitly state it as such.

> *"The collective attitude is one of maintaining and respecting data"*

> *"We deal with survey data, so most of the emphasis is centred around ensuring that no personal respondent information is shared in an unsecure manner."*

It is expected that organisations will take information and data security seriously to some extent. Thereby, the assumption is made that organisations do acknowledge the importance of information and data security although there is not in all instances sufficient evidence available from respondents' answers to motivate this statement. Only 5 respondents, which is the minority, showed unsurety regarding their organisation's security culture. Some respondents perceive their organsisation to share a security culture that lean towards being more "relaxed" than being serious.

> *"its very chilled passwords are shared openly"*

> *"We're not too strict about it, but we are aware of it"*

In the occasion of any form of detected threat or computer related security breach (Q5), most respondents stated in their answer that they are required to escalate the matter. This is mostly done by reporting or refer the threat/incident to either the relevant IT security or management. Similar to the responses for Section B1 question 4, many respondents stated the immediately quarantine or isolation of the infected device. From responses, this is done by shutting the device down, completely isolating the device or disconnecting from any network or connection. In general, their actions refer to the complete refrainment of interaction with the device until management or authority can investigate the breached device.

> *"Escalate to the manager and isolate the device(s)."*

> *"Immediately tell helpdesk and disconnect from internet"*

Only two respondents show indication that they will take the matter in their own hands to remediate the threat. Eight respondents show unsurety on how to react in such a circumstance or do not provide a useful response. It is thus clear that as seen in the majority of answers in question 4, a high sense of awareness and alertness of security risks and breaches are visible

within organisations. When respondents were asked whether they receive any form of security training or education from their organisations (Q6), a surprisingly larger number (15 respondents) stated an absence of training received. From those respondents who indicated that they do receive some form of training, the answers were sorted as follows. Those who receive training by participating in workshops or physical training sessions. Those who receive training in the form of readable material or informal talks that help to raise awareness. Those who stated that they only received training on once newly appointed and lastly, those who confirmed that they received training, but gave no specific indication as to how they receive this training or education. Also, many participants indicated that they received training on a regular basis, while some others may receive training once a year.

> *"Yes. Constant security updates, training courses, onboarding for new staff and frequent security talks."*
>
> *"regular awareness emails"*
>
> *"Yes, there are also regular phishing test messages sent to check awareness."*

The majority of respondents organisation some form of security training or education for employees, regardless of what form the training occurs in. Respondents were also asked whether their organisation requires them to make use of additional security measures to secure their work-related accounts (Q7). Both with this question and questions Q5, the focus is on requirements placed from the organisation itself. Again, a surprisingly larger number of respondents (16) respondents stated that they do not make use of additional security measures, assumably other than a standard username and password for accounts. The rest of the respondents confirmed that they do make use of additional security measures. Most of these respondents stated that they do make use of multi-factor, also known as 2-Factor authentication for accounts. Only 10 respondents gave confirmation of the usage of additional security measures did not provide an indication of the specific type of additional measures they use. This finding corresponds with the findings of Mcanyana et al., (2020) where 50% of the respondents were not aware of multi-factor authentication or its associated benefits.

Respondents were also asked regarding the availability and accessibility of IT/support groups within their organisation (Q8). Only one respondent stated that they do not have any IT or support group in their organisation and two respondents gave no answer to the question. Out

of the respondents who answered “Yes” to the presence of a support group, the majority (25) gave indication that their support group are easily accessible. Those respondents who directly stated in their answer that support groups are easily accessible or describe their accessibility through Emails, messaging, telephonically or onsite help/service desks were considered to have easily accessible support groups.

> *“Yes working from home made everything easy contact them via audio and give them access to the problem”*

> *“Yes, all employees have direct access to various levels of support”*

Only 5 respondents stated that their IT/support groups are not very easily accessible, mainly because of the long waiting period after they have logged a request for support. 18 respondents stated that they do have an IT/support group in their support group but gave no indication of their accessibility. A visible trend among many respondents' answers is the use of a logging or ticketing system to log request for support. As already mentioned, it appears that respondents who experience a logging or ticketing system are dissatisfied due to that waiting period of a request is logged.

> *“We have an IT support group but as mentioned previously, it works with a ticketing system and they take a very long time to address any issues that we have”*

The last question of this section as well as for the entire survey, respondents were asked about their access security of their organisation’s information system, specifically from an offsite location (Q9). Surprisingly, 8 respondents stated that they do not have access from an offsite location. The remainder of respondents stated that they do have access. These respondents were categorised between those who make use of a VPN (27), those who make use of other methods to connect to the information system or portal (5) and those who confirmed that they do have access but gave indication of their method of connection (3). It is thus clear that from responses for question 7 and 9, a high level of awareness and readiness among the respondents in terms of safe connection and data transfer between respondent and the organisation.

Chapter 5

Discussion

5.1 General findings

The purpose of the survey study was to investigate the overall level of security awareness and response to threats that are present and that anyone may encounter within the digitised environment. Additional emphasis was placed on the actual observable behaviour of employees when exposed to certain stimuli, in this case, any form of security threat. The information found from the investigation aided in gaining a perception of the overall security posture that is already present within the digital workforce. Additionally, this investigation included what the type of potential risky behaviour is and how to prevent or remediate the threat that may arise from such behaviour.

As previously discussed, the survey study consisted of three separate sections, all which contribute to the overall understanding of the security posture of the sample. With regards to the gender distribution across the various questions for Section A, there is no specific trend indicating a significant variation between male and female respondents. Thus, this confirms the assumption that there would be no significant various between gender groups. The analysis of Survey Section A suggests that the majority of respondents' answers show security and risk awareness in their use of information systems. This awareness can be seen in answers to questions across all four subsections. However, it is evident that a few respondents (the minority) show actions that tend to be less secure or favorable such as with regards to password management 11 respondents (19,6%) never update their account passwords. Additionally, it was found that 9 respondents (16,1%) create accounts with easy rememberable passwords, while 31 (56,4%) use repeatable passwords for various accounts. With regards to device and data security, just below half of respondents do not use anti-virus software on all their devices and four respondents never back-up any of their data. 14 Respondents either do not know how to take security precautions or do not feel the need to take security precautions when working with technology. 24 Respondents do make use of their work-related Email accounts for personal matters and generally a high admittance to accidentally sending an Email to the wrong

recipient (30 respondents). Similar results are found for the usage of work-related devices for personal purposes. A high unattendance rate of work-related devices in the workplace was found (34 respondents). This number of respondents contradicts the amount (14) who do not take precautions when working with technology, as leaving a device unattended could be regarded as unsafe. It is possible that this behaviour is influenced by the level of trust an employee has in the safety of the organisation's working environment. Lastly, with regards to the EFT purchases, over half or respondents make EFT purchases directly from a third-party website, which is described in the literature review as extremely risky (Business Insider SA, 2020). Finextra, (2020) emphasises the importance of awareness and education of both the risks and benefits of electronic payments. This is especially applicable in the global economy where online crimes are drastically rising because of an increase in online transactions. In conclusion, generally in Section A, risky behaviour is evident in the minority of answers. However, there are exceptions for some questions, where a greater number of respondents showed risky behaviour in their answers.

The aim of Survey Section B was to identify certain risks that arise from respondents' behaviour when exposed to certain potential threats, which represents stimuli. Both the response to the exposure to stimuli within the organisation as well as offsite from the organisation was investigated the broaden the scope of exposure to threats. Within the analysis of this survey section, it is immediately evident that most respondents already portray a strong sense and awareness of security threats and how to react accordingly. This is visible in both subsections of the survey. With regards to stimuli exposure within the organisation (Survey Section B1), it appears that when respondents are situated physically within the organisation, the evidence of risky behaviour decreases significantly. This may be as a result of respondents being more cautious and aware when they are at work from potentially being under surveillance. Additionally, although not investigated, a physical organisational environment may stimulate focus that could improve caution and awareness as opposed to being offsite where the influence of distraction is present. The higher secure behaviour could also be because of infrastructure provided by the organisation for onsite use such as internet connectivity and electronic devices. None of the respondents indicated that they were expected to use their own data connection for onsite work-related purposes. However, when respondents are situated at an offsite location (Section B2) and in need of a data connection, thereby creating the need for self-provided data, risky behaviour starts to occur. It was found that many respondents will make use of self-provided data or public Wi-Fi networks to carry out work related activities, without the

mentioning or consideration of the risks associated with such actions. The majority of respondents will acknowledge the importance of secure connections and thus in many cases state the usage of VPNs to secure the connection.

It is interesting to observe that some respondents neglected to provide an adequate answer for some questions in Survey Section B. When asked how they would respond to a specific cyber-threat, the respondents would answer that the cyber-threat in question had never happened to them before. The reason for this type of answer may be that the respondent does not know how to behave in the event of the cyber-threat, or the respondent did not understand that the question involves a hypothetical cyber-threat. Therefore, the respondents were asked to give their hypothetical response in this situation, regardless of whether they have personally experienced the cyber threat or not. Another reason for giving this type of answer may be that the respondent believes that the cyber-threat does not apply to them and denies answering the question.

Most respondents show a strong sense of awareness and caution. The identified risks only pose a threat when an employee can be easily deceived/scammed to provide access to sensitive information. The more an employee has access to a certain level of data or information system, the greater the loss or damage can occur from the infiltration of the data or information system. Thereby, access and authority are identified as a very important factors for the security of information and data. As it is found that many of the response strategies as seen in Table 4.1 relate to education, access restriction and training, it should be a focal point in every risk management plan. This enables employees to quickly identify an attempt by a scammer, nefarious website, advertisement, or link and react appropriately.

After applying the risk assessment formulas presented and discussed in the analysis section, all the identified risks had a probability of occurrence percentage lower than 15%. In combination with the impact assessment of the worst possible outcome for the organisation, that is the infiltration of malware, all risks receive a total score of 5 and a rank of 1. This would in return require a risk response of “Accept” as described by Blackman (2015) for low risks. However, due to the significant financial impact that malware can have on organisations, even the slightest human error or mistake should be prevented. It is estimated that the total recovery cost for South African organisations is R3 871 010.33 on average, Sophos (2020). Thus, organisations should consider every potential action that an employee may take that could cause a security breach, regardless of the low probability of occurrence.

It was found in the literature that South African digital workers portray a high security posture as well as research showing that South Africa is in the top five global countries at preventing data encryption from malware (Sophos, 2020). Accenture (Mcanyana et al., 2020) provides information that would prove South Africa's defense capabilities otherwise. (Mcanyana et al., 2020) states that cybersecurity in South Africa is not on par or as robust as other global countries. Additionally, (Mcanyana et al., 2020) continuous that because of South Africa's substandard security posture, various threat actor considers South Africa as a malware testing ground. These threat actors can thus use test tools and techniques on South Africa, before attempting the deployment on more sophisticated countries.

The aim of survey Section C was to investigate respondents' personal perceptions of digital risks, the importance of information and data security, as well as their view on the security culture within their respective organisations. This qualitative analysis, in addition to the analysis of Section A provided more context for the formulation of the general perception of the security posture already portrayed by the respondents and their respective organisations. From the analysis of this section, similar insights are gained regarding the overall level of security and awareness among the respondents and digitised organisations. The majority of respondent's show a good understanding of the term "digital risks" as well as of the importance of data and information security in modern organsisations. Only two respondents out of 56 did not show interest in the importance of the topic. Most respondents who acknowledged the importance of the topic provided motivations that ranged between the repercussion from the lack of ample security, or the value gained from protection of sensitive information. With regards to the understanding of the term digital risks, the majority correctly associated digital risks to those introduced by conducting business in the digital environment, data being digitally used and stored, the usage of technology or any form of cybercrime. Only 7 respondents show unawareness of the term. The remainder of questions in this section focused on respondents' perspective of their organisations, with the aim to gain insight into the security culture, requirements, and expectation within the workplace. It was found that 15 respondents do not receive adequate security training or education from their organisations. This raises a big concern, as previously mentioned that training and education should be an integral part of any risk management plan. This seemingly high number of respondents who do not receive adequate security could contribute to explaining why there is risky behaviour found by several respondents' answers throughout the entire survey. With regards to perceived organisational security culture, it was found that most respondents work in organisations that have a strict

view on information and data security. Only a few cases did respondents mention a relaxed security environment.

From those respondents who indicated a relaxed security environment, one respondent stated that the security measures taken in the organisation differ from person to person. This finding aids in the confirmation that although an organisation may portray a strong security culture, the acts of one person can jeopardise or put the entire posture at risk. To investigate security culture in more depth, questions were asked regarding the required response to breach detection, what additional security measures are used to secure accounts, information system access and security, support group availability and accessibility. It was found that all the beforementioned organisational factors contribute positively to the general security posture of digitised organisations. Additionally, it was found that regardless of the respondents' level of experienced stress in the workplace, stress does not appear as a determining factor of technology proficiency.

Overall and in general, adequate, and responsive support groups are evident within organisations. Additionally, organisations do require employees to make use of multiple layers of security for the safeguarding of accounts. In addition, they require timely escalations of security breaches and equip employees to safely establish networks connections. This is mostly done using VPN's. This general conclusion is made through the consideration that most of the responses are positive in nature and promotes behaviour that contributes to the strengthening of the security posture of respondents as well as their respective organisations.

5.2 Discussion of research questions

Research Question 1 asks whether current risk management strategies used in companies effective at managing security risks and threats. From the results of this study, there is no evidence to support that organisations do use adequate risk management strategies. However, with regards to Research Question 1, adequate risk management strategies do not fully impede the occurrence of human error as for each investigated potential scenario, risky behaviour is still evident regardless of the overall impression.

Research Question 2 asks what the strengths and shortcomings are found among digital risk management strategies/frameworks within literature. It was found in the literature review that the studies share the same base formula for risk assessment. The base formula used to assess an identified risk is through the combination of the impact the risk may have financially on an organisation and the probability that a specific threat may occur. However, studies provide their own unique perspective on how to determine the impact and risk of threats, all of which can be determined uniquely by any organisation. These formulas are only effective for risk assessment when actual financial information is such as the costs of information and technological assets which may be the target of a cyber threat. Only once such information is available can the organisation utilise the formula provided to effectively conduct a risk assessment plan. For the case of this study and the limitation of the methodology only investigation employees and not organisations directly, there is an absence of financial information. As a result, this study used general financial information provided by research to for the assumption of the impact and probability of identified risks and threats as seen in the analysis section. In answering RQ2, it is clear that organisations are highly risk and threat aware and do enforce a security culture that aims to minimise security risks that may lead to potential threats or breaches.

Research Question 3 asks whether modern digitised organisations are aware of the impact and vulnerability of the workforce related to cyber threats. As this study was only limited to the investigation of employees and not organisations directly, assumption regarding organisations were made from the insight gained from respondents' answers. Organisational security and risk awareness are roughly estimated based on how respondents perceive the security culture. From the overall finding that organisations indeed have high expectations of employees regarding security protocols and education, the assumption is made that organisations as entities are highly aware of the vulnerability posed by employees. This could potentially be the reason why employees perceive their organisation portraying a strict and serious security culture as they only want to prepare and educate employees as adequately as possible.

Research Question 4 asks whether digitised companies implement risk management strategies that cater for or mitigate potential threats caused by the workforce. The same assumptions that were made to answer RQ3 are used to answer RQ4. From the overall impression of the security from the majority of respondents' answers as well as their own perception of their respective organisations, the assumption is made that digitised companies do implement risk management strategies that cater for or mitigate potential threats caused by the workforce.

Research Question 5 asks whether the average worker possesses the level of knowledge, skill, and risk awareness to implement adequate security measures in their day-to-day activities within organisations. The general conclusion was made that employees and their respective organisations show an overall strong security posture and risk awareness. This conclusion was formulated with the consideration of various aspects of security culture that are used to define the overall security posture of employees and organisations. In answering Research Question 5, respondents' answers across all three sections of the survey were considered in its entirety.

Research Question 6 asks whether environmental stimuli-behaviour investigation effective enough at gaining an understanding of behaviour when potentially exposed to cyber/digital threats. According to the Behaviorist/behavioural Learning theory, behaviourism is only concerned with observable behaviours in response to environmental stimuli (Dr McLeod, 2020). The Behavioral Learning Theory and the Social Learning Theory are rooted in similar concepts. Both the Social Learning Theory and the Behavioral Learning Theory agree that external, environmental factors influence behavior. However, the Social Learning Theory improves on the Behavioral Learning Theory by suggesting that behaviour is also shaped by internal psychological processes. Therefore, it is believed that the Social Learning Theory provides a more comprehensive understanding of human behaviour. However, for this study, the subject of interest is how employees interact with and respond to cyber threats. Cyber threats may be regarded as an external, environmental stimulus. Therefore, the Behavioral Learning Theory is adequate in providing insight into the behavioural patterns of the respondents when exposed to cyber threats. For future research, the Social Learning Theory may be utilised to understand the influence of both internal psychological processes and external, environmental stimuli. It is expected that the Social Learning Theory will provide a more comprehensive understanding of behaviour by providing insight into the psychological motivations behind behaviour.

To answer Research Question 6, the Behavioral Learning Theory provided insight in investigating respondents' stimuli-response behaviour when potentially being exposed to cyber threats. It was observed that the respondents show risky behaviour in response to various cyber threats. It is believed respondents show risky behaviour as a result of being unconcerned with consequences when exposed to potential threats. Another reason for the risky behaviour may be that the respondents lack an understanding of how risky their behaviour in response to the

cyber threat is. The final possible reason for the risky behaviour is the lack of knowledge and skill of how to respond to the threat in the correct manner. These risky behaviours include the usage of public Wi-Fi networks when connecting to organisational networks, the sharing of user credentials, not updating or postponing anti-virus software, clicking on random pop-up advertisements etc. In every stimuli-response scenario, as seen in Survey Section B, there were respondents who portrayed risky behaviour. There can be concluded that within the sample, there a number of respondents showing risk-prone behaviour; however, most respondents portray a strong security posture and risk awareness. The Behavioural Learning Theory is found assisted in gaining insight into the behavioural patterns of employees when they are confronted with cyber threats. The findings support that human-factor security is an essential consideration in the discourse of cyber threats. However, the psychological motivation behind behaviour is not clear from the findings of this study. As such, the findings suggest Social Learning Theory may be utilised in future to understand the reason for the variability in behaviour among respondents' answers. This supports the foundation of the Social Learning Theory, that there are indeed internal psychological processes that influence behaviour. As described in the literature review, there are many psychological as well as external influences on behaviour. An important factor in determining behaviour is the nature of the security posture of the respondents' respective organisations' security culture. A lack of a strong security posture is visible within the risk-prone respondents. This leads to the suggestion that those respondents with a strong security posture are more informed, aware, and trained on security risks show more risk-averse responses to certain stimuli or threats.

Chapter 6

Conclusion

The purpose of this study was to investigate human-factor security within digital risk management. Human-factor security was investigated to gain an understanding of the behaviour of employees when presented with cyber threrats. The behaviour of employees was examined to identify and quantify the security risks that their behaviour introduced. Thereafter, a risk management plan was developed. The purpose of the risk management plan is improve risk management in digital organisations. The literature review provided information on the existing risk identification and management frameworks, as well as the cognitive science behind human behaviour relating to threat exposure. This goal of this investigation was to gain an understanding of its level of usefulness, success, and whether there is a shortage of emphasis on human behaviour in risk management. Existing literature within the field of digital risk management aided in the formulation of a risk management plan. However, none of studies in the existing literature focused exclusively on the impact that of human-factor security. Additionally, multiple studies provide insight on the influences of human behaviour that could aid in the understanding of the causes of human vulnerability and susceptibility to cyber threats. Thereby a qualitative study was conducted to investigate human behaviour on three fronts. Firstly, the focus was on existing level of security and risk awareness in the digital workforce. Secondly, the focus is on behavioural responses through the exposure of environmental stimuli, by utilizing the Behavioural Learing Theory. Lastly, the workforces' self-perception on the prominence of digital risks and security as well as on the perceived security culture within organisations.

This study provided qualitative research whereby a survey was deployed to investigate human behaviour when exposed to cyber threats as well as the security posture among the digital workforces. From the review of risk assessment frameworks and formulas presented by studies, a general formula was developed. This formula considers the factors that were ubiquitous across the various formulae. Additionally, this formula was used to assess the risks identified among stimuli-response behaviours. Not only does the utilisation of the formula determine the effectiveness of its use, but also used to seek out the threats that arise from risk-prone employees. Additionally, the survey investigation was used to determine the overall security

posture evident in employees. This was determined by the level of risk and threat awareness as well as knowledge of digital risks and how the usage of technology threatens the integrity of organisational information and data. The data gathered that investigated the security posture of respondents as well as their respective organisations were analysed through a thematic analysis approach. The results from this analysis were grouped into various themes with each main theme contributing to the perception of existing security posture portrayed by the respondents themselves and their respective organisations. The overall organisational security posture was determined from the combined perception through the eyes of the workforce.

The literature review provided valuable findings on risk assessment and management, human cognition on and influences of behaviour as well as from a qualitative investigation of stimuli-response behaviours. Firstly, this study confirms that, regardless of the level of sophisticated technology used in organisations, the technology is just as vulnerable as the person operating or interacting with it. This coincides with the findings from Ani et al., (2019) stating that an organisation is just as strong as its weakest link. Secondly, adding to the first finding, regardless of how sophisticated technology may be or how strong a organisations security posture is, it takes one mistake or human error to jeapordise the integrity of the entire organisation. It is also important to appreciate that risks with a high impact should be regarded as dangerous, even the risk is associated with a low likelihood. Thereby, organisations should maximise their efforts to prevent an occurrence of the risk. It was found that a breach occurrence is highly likely to occur in most organisations, at least once during some point of the orginisation's existence (Hope, 2021). Organisations should not overlook the role of human-factor security cyber threat prevention. Additionally, orginisations should aim to continuously promote security and threat awareness. The repercussions and potential financial damage can be on large scales and can even lead to an orgnisation's permanent shutdown. Through continuous training, education and threat awarenesss among the workfore, organisations can only strengthen their security posture and decrease the probability of a threat occurrence as far as possible.

The findings from this study suggest that observable environmental stimuli-response behaviours do provide insight into understanding human error in response to digital threats. Further investigation utilising the Social Learning Theory that includes personal psychology traits in combination with stimuli responses is needed to provide deeper insight into human behaviour in response to cyber threats.

The findings from this study contribute to the body of knowledge on risk management as well as human behaviour in the cyber security domain through a qualitative study on an authentic dataset. Additionally, security and risk managers can utilise these findings to gain insight into human behaviour and susceptibility to cyber threats. This insight can be utilised potentially improve risk management and maximise the organisations' security posture.

6.1 Limitations

From this project and analysis several limitations were identified in the following aspects of the study:

Sample size: Due to the usage of a small sample size, results were mainly produced through generalisation. The age variable from the survey respondents was discarded from analysis due to the limited number of responses and uneven distribution of age. The small number of total respondents of the survey serves only useful for a qualitative study. A larger sample size is needed in order to incorporate a quantitative study into the project. When calculating averages with small sample sizes, large deviation in single respondents' answer may skew the results and provide an inaccurate representation of reality. The absence of statical analysis is a result of the qualitative nature of questions used in the survey.

Self-reported data: All data captured and analysed were provided by respondents of the survey's answers. Regardless of the anonymity and voluntary nature of data collection, it was found that many respondents did not provide quality motivation or explanation for answers. This affects the accuracy of the analysis. As a result of the limitation of self-reported data used, concepts that were investigated such as organisational security culture and posture, could only be formulated by the limited information provided by respondents. This may lead to a finding that represents a misunderstanding of alignment between the perception of cultures as seen by the employees and the organisation distinctively. Respondents can provide personal biased perceptions with regards to experience within their organisations, which may be viewed differently by their employer. Further investigation with a more personal approach such as an interview would provide the necessary background in order to understand respondents' personal biases.

Research focus: With the focus only on human behaviour when exposed to environmental stimuli, as well as personal perception of security and risk awareness, this study did not investigate many other factors that may influence behaviour. The Behavioural Learning Theory was used as the main factor which steered the direction of the survey and study. It was found that further investigation of other factors that may influence behaviour such as personal psychological traits is needed, as required by the Social Learning Theory. As a result of the Behavioral Learning Approach, the survey investigation was only limited to an initial response when exposed to certain environmental stimuli. No further investigation was conducted, such as on emotional or mental reactions that may have been triggered because of exposure to stimuli. Such additional investigation may have led to insight into the understanding and cause of certain behaviours.

It would be interesting to know what personality traits, if any, may be associated with an inclination to be risk averse, or partake in risky behaviour.

6.2 Future Research and recommendations

From the execution of this project and the identification of limitations, the recommendations and suggestions for future research follows below.

This study's investigation focuses solely on security awareness and behaviour in relation to organisational information and data security. However, human behaviour as a single factor is only one of many factors that defines the overall security posture of an organisation. An organisation's security posture and readiness to cyber threats cannot be derived only from the overall posture of the workforce. Due to the inevitability of a cyber attack, the organisation's ability to recover from such an attack holds significant weight. Sophos (2020) highlights that cybersecurity insurance aids in the recoverability of an organisation after a ransomware attack. It was found that from all companies that had data encrypted from a ransomware attack, 94% of cases where the ransom was paid the cost was covered by insurance. Additionally, Balbix (2021) highlights five factors that define an organisation's security posture. These factors include existing protection controls and processes, attack detection and containment, attack recoverability, the level of automation in the organisation's security program and level of visibility in the organisation's asset inventory. There can be seen that the human employee has

a role in each of these factors. Thus, human-factor security needs to be investigated in order to determine an organisation's security posture. It is proposed that human behaviour should be investigated in greater detail, as to consider the human worker's role in the above-mentioned factors.

It is assumed that respondent's answers are subjective to their own perceptions of their security posture as well as their respective organisation's posture. The possibility that subjectivity in the answers could misrepresent reality. Thereby the question arises that if respondents' perception of their personal and their organisations security posture align with how security officials from the organisation perceive it. Thus, in order to fully determine the security posture of an organisation, additional investigation is needed with the focus on security officials in order to determine alignment of perceptions and expectations between organisation and employee. The utilisation of interviews as data collection methodology would allow for more meaningful insights and will also improve the quality of data collection. Interviews would prevent the collection of meaningless answers as seen with the usage of anonymous surveys.

As it was concluded that The Behaviorist Learning Theory does not provide adequate support for the understanding of human behaviour, further investigation with the use of The Social Learning Theory could be utilised to broaden this understanding.

6.3 Conclusion

Human-factor security is of great importance when investigating cyber threats in digitised orginisations. Human behaviour is determined by a combination of both the understanding of personal psychological influences and the exposure to environmental stimuli. This study provided insights on human behaviour when exposed to various cyber threats. From the survey, behaviour associated with high security risks were identified. An appropriate risk management plan was developed to address the identified risks. The findings from this study provide great benefit to almost every aspect of an organisation's security culture. The human employee is at the forefront of every facet of cyber security. It is crucial that organisations take every necessary step to prepare and promote security and risk awareness in the workforce. With the rapid improvement and sophistication of modern cyber-attacks, it is nearly impossible for organisations to completely prevent every attack. Cyber-attacks and breaches have an extremely high probability of occurrence. Therefore, organisations should appreciate the

importance of an effective risk management plan that addresses human-factor security. It only takes one minor human mistake or error that leads to an organisation's downfall.

Appendix A

Survey Section A

Organisational related questions
Questions in this section require you to only select the best suitable answer.

Q1: Does your organisation have a Log-In system in able for you to do your work?
- YES
- NO

Q2: How safe do you perceive your personal information to be on your organisation's information system? Choose your level of trust.
- I trust my organisation fully
- I feel neutral about my organisation
- I do not trust my organisation with my information

Q3: How safe do you perceive your interaction with technology in your organisation (such as working safely on a work computer or connecting to company Wi-Fi)?
- I perceive my interaction with technology to be very safe
- I feel neutral about the safety of my interaction with technology
- I am not sure about the safety of my interaction with technology

Q4: Do you use personal devices, such as smartphones or computers, on your organistion’s networks (Wi-Fi)?
- YES
- NO

Q5: How easy do you find your organisation's information system and technology to use?
- The system is very easy to use
- The system is somewhat easy to use
- The system is sometimes difficult to use
- I struggle to use the system

Q6: Are you allowed to take your company device(s) home/off site?
- YES
- NO

Password management:
Questions in this section require you to only select the best suitable answer.

Q7: How regularly do you change your passwords?

- Weekly
- Monthly
- Once every 2-3 months
- Once every 3-6 months
- Yearly
- Never

Q8: How would you describe the complexity of your passwords?

- I use a password that is easy to remember
- I use semi-complex passwords, but still able to memorise without difficulty
- I use a complex password

Q9: Do you create new passwords when creating new accounts or use repeatable/known passwords?

- I use known/repeatable passwords as its easy to remember
- I use a new password for each account

Protection of devices

Questions in this section require you to only select the best suitable answer.

Q10: Do you use anti-virus software on your electronic devices?

- I use anti-virus software on all my devices
- I use anti-virus software on some devices
- I do not use anti-virus software

Q11: How regularly do you update your anti-virus software?

- Weekly
- Monthly
- My anti-virus client updates automatically
- Never

Q12: Do you regularly backup your data (such as messages, files, work documents etc.)?

- Regularly
- Sometimes
- Never

Overall technology proficiency and awareness

Questions in this section require you to only select the best suitable answer.

Q13: How vigilant and cautious are you when working with technology?

- I always check to see if what I am doing is safe
- I do not feel it is necessary to take precaution when working with technology
- I do not know how to check if my interaction with technology is safe

Q14: Do you ever use your work computer/device for anything other than work related activities?

- Always
- Sometimes
- Never

Q15: Do you use your work Email for personal purposes? For e.g. subscribing to a newsletter with your work Email.

- Always
- Sometimes
- Never

Q16: Do you ever leave your work PC or mobile device unattended at work?

- Always
- Sometimes
- Never

Q17: When you need to read terms and conditions when signing up for something online, do you ever select “I accept” without proper background reading?

- Always
- Sometimes
- Never

Q18: Have you ever accidentally sent an Email to the wrong recipient?

- Frequently
- Sometimes
- Never

Q19: Do you make online purchases via EFT’s? If yes, please select your method of payment. If not, please select the third answer.

- I make EFT's directly on the website from where I want to make a purchase
- I make an EFT to the receiver of the payment directly from my banking app
- I do not make use of EFT's for payment

Survey Section B1

Q1: How would you respond when you receive an Email from an unknown sender requesting personal information in your work Email inbox?

Q2: How would you respond when you are about to visit a website on your company device and the browser warns you that the website is unsafe?

Q3: How would you respond when your workstation prompts you to do a system update or any other update?

Q4: How would you respond when your workstation warn you that a virus has been detected on your computer?

Q5: How would you respond when you suddenly experience the company Wi-Fi to be slow and you need a better data connection in order to complete an important task on time?

Q6: How would you respond when working on your work computer and an advertisement pops up relating to something or product you recently browsed?

Q7: How would you respond when your current device is connected to company Wi-Fi and a social media notification pops up?

Q8: How would you respond when prompted by a colleague(well known or not) to share access credentials for any particular reason?

Survey Section B2

Q1: How would you respond when you receive a phone call requesting personal information of either you or your organisation claiming to be from your company or someone you know?

Q2: How would you respond when you need to connect to your organisation's information system, but you are at an offsite location?

Q3: How would you respond when you receive random friend requests on social media from persons claiming to be your friend or someone you know?

Q4: How would you respond when you need an internet connection on your company device at an offsite location and public Wi-Fi networks are available?

Q5: How would you respond when you realise you have sent an Email to the wrong person that contains classified/personal business information?

Survey Section C

The aim of the questions in this section is to gain a grasp of your own perceptions on digital risks, your own security posture as well as your perceptions of the security culture within your organisation.

Q1: Do you believe that information and data security plays an important role in any company? Please motivate your answer.

Q2: What is your perception or understanding on the term "digital risks"?

Q3: How would you describe your average stress level at work? Do you feel that your stress level influences your proficiency with technology? If so, how?

Q4: Please describe the collective attitude/ culture in your company toward information and data security.

Q5: How do your organisation require you to respond in the event of a detected threat or any security breach?

Q6: Does your company provide any training or education on digital risks or secure practices? If so, please specify.

Q7: Does your company require you to use additional measures of security, such as two-factor authentication or passphrases for work related accounts? Please specify.

Q8: Do you have an IT/Support group which you can contact within the organisation and can you communicate with them easily? Please specify.

Q9: Do you have access to your company's information system or portal from an offsite location? If yes, do you use a VPN or any other methods to secure your connection? Please specify.

Bibliography

ageUK. (2021). *Phone Scams*. https://www.ageuk.org.uk/information-advice/money-legal/scams-fraud/phone-scams/

Allen, N. (2021). *Africa's Evolving Cyber Threats*. https://africacenter.org/spotlight/africa-evolving-cyber-threats/

Ani, U. D., He, H., & Tiwari, A. (2019). Human factor security: evaluating the cybersecurity capacity of the industrial workforce. *Journal of Systems and Information Technology*, *21*(1), 2–35. https://doi.org/10.1108/JSIT-02-2018-0028

Ao, S. I., International Association of Engineers, WCECS (2008.10.22-24 San Francisco), & World Congress on Engineering and Computer Science (2008.10.22-24 San Francisco). (2008). *WCECS 2008, World Congress on Engineering and Computer Science, San Francisco, USA, 22-24 October, 2008*. IAENG International Association of Engineers.

Bada, M., & Nurse, J. R. C. (n.d.). *The Social and Psychological Impact of Cyber-Attacks*.

Baker, K. (2021). *THE 11 MOST COMMON TYPES OF MALWARE*. https://www.crowdstrike.com/cybersecurity-101/malware/types-of-malware/

Balbix. (2021). *What is Security Posture?* https://www.balbix.com/insights/what-is-cyber-security-posture/

Blackman, A. (2015). *Effective Risk Management Strategies*. https://business.tutsplus.com/tutorials/effective-risk-management-strategies--cms-22887

Boblin, P. (2018). *Why People Don't Update Their Computers*. https://www.techzone360.com/topics/techzone/articles/2018/07/13/438785-why-people-dont-update-their-computers.htm

Bojanc, R., & Jerman-Blažič, B. (2013). A quantitative model for information-security risk management. *EMJ - Engineering Management Journal*, *25*(2), 25–37. https://doi.org/10.1080/10429247.2013.11431972

Briggs, P., Blythe, J., & Tran, M. (n.d.). *Using behavioural insights to improve the public's use of cyber security best practices*.

Brown, E. (2020). *Over half of the calls people receive now are spam*. https://www.zdnet.com/article/over-half-of-the-calls-people-receive-now-are-spam/

Business Insider SA. (2020). *Beware of 'instant EFT' when buying online, regulators warn – you risk a great deal*. https://www.businessinsider.co.za/reserve-bank-fsca-warns-against-instant-eft-for-online-shopping-2020-11

BusinessTech. (2021). *Cyber threats on the rise in these industries in South Africa*. https://businesstech.co.za/news/cloud-hosting/502645/cyber-threats-are-on-the-rise-in-these-industries-in-south-africa/

Capodagli, S. (n.d.). *DIGITAL RISK MANAGEMENT AND RESILIENCY – PART ONE*. Retrieved June 3, 2021, from https://enterpriseriskmag.com/digital-risk-management-and-resiliency-part-one/

Check Point. (2021). *Mobile Security Report 2021. Insights on Emerging Mobile Threats*. https://pages.checkpoint.com/mobile-security-report-2021.html?utm_source=blog&utm_medium=cp-website&utm_campaign=pm_wr_21q2_ww_mobile_security_report_2021

Chmura, J. (2016). THE IMPACT OF POSITIVE ORGANISATIONAL CULTURE VALUES ON INFORMATION SECURITY MANAGEMENT IN THE COMPANY. *Journal of Positive Management*, *7*(1), 87. https://doi.org/10.12775/jpm.2016.006

Chu, M. (2021). *What Happens If You Open Spam Email? 4 Dangers To Your Account*. https://dataoverhaulers.com/open-spam-email/

CMIT Solutions. (2021). *Fake Social Media Friend Requests Represent Latest Ploy by Scammers*. https://cmitsolutions.com/blog/fake-social-media-friend-requests-represent-latest-ploy-scammers/

Connolly, L. Y., Lang, M., Gathegi, J., & Tygar, D. J. (2017). Organisational culture, procedural countermeasures, and employee security behaviour A qualitative study. *Information and Computer Security*, *25*(2), 118–136. https://doi.org/10.1108/ICS-03-2017-0013

Conteh, N. Y., & Schmick, P. J. (2016). Cybersecurity:risks, vulnerabilities and countermeasures to prevent social engineering attacks. *International Journal of Advanced Computer Research*, *6*(23), 31–38. https://doi.org/10.19101/ijacr.2016.623006

Cook, S. (2021). *35+ Phone Spam Statistics for 2017 – 2021*. https://www.comparitech.com/blog/information-security/phone-spam-statistics/

Corporate Finance Institute. (2021). *Business Risk. A threat to the company's ability to achieve its financial goals*. https://corporatefinanceinstitute.com/resources/knowledge/finance/business-risk/

Costello, K. (2019). *Risk management programs must address a widening array of IT threats associated with digital business.* https://www.gartner.com/smarterwithgartner/digital-business-requires-integrated-risk-management/

CPNI. (2021). *Security Culture: What type of security culture do you have, and does this support the demonstration of the right security behaviours?* . https://www.cpni.gov.uk/security-culture

Cvetićanin, N. (2021). *What's On the Other Side of Your Inbox – 20 SPAM Statistics for 2021*. https://dataprot.net/statistics/spam-statistics/

da Veiga, A., Astakhova, L. v., Botha, A., & Herselman, M. (2020). Defining organisational information security culture—Perspectives from academia and industry. *Computers and Security*, *92*. https://doi.org/10.1016/j.cose.2020.101713

Data Spotlight. (2020). *Scams starting on social media proliferate in early 2020*. https://www.ftc.gov/system/files/attachments/blog_posts/Scams%20starting%20on%20social%20media%20proliferate%20in%20early%202020%20/data_spotlight_oct_2020.pdf

de Oliveira, D. (2020). *Digital Risk: What It Is And How to Manage It in Your Org*.

Delaney, R., & Delaney, R. (2015). *The Challenges of Integrating New Technology into an Organization* (Vol. 25). http://digitalcommons.lasalle.edu/mathcompcapstoneshttp://digitalcommons.lasalle.edu/mathcompcapstones/25

Deloitte. (2018). *Managing Risk in Digital Transformation Risk Advisory Managing Risk in Digital Transformation Managing Risk in Digital Transformation*.

Dr McLeod, S. (2020). *Behaviorist Approach*. https://www.simplypsychology.org/behaviorism.html#:~:text=The%20Behaviorist%20Approach,a%20response%20to%20environmental%20stimuli.

Dutta, P. (2020). *5 Risks of Password Sharing at Work*. https://www.kratikal.com/blog/5-risks-of-password-sharing-at-work/

Evans, M., Maglaras, L. A., He, Y., & Janicke, H. (n.d.). *Human Behaviour as an aspect of Cyber Security Assurance*.

Finextra. (2020). *SARB issues dark warning over screen-scrapers on Black Friday*. https://www.finextra.com/newsarticle/37032/sarb-issues-dark-warning-over-screen-scrapers-on-black-friday

Fruhlinger, J. (2018). *What is WannaCry ransomware, how does it infect, and who was responsible?* https://www.csoonline.com/article/3227906/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html

Furnell, S. M. (2005). *Considering the Security Challenges in Consumer-Oriented eCommerce*.

Gardiner, M. (2021). *E-commerce and the dangerous rise of screen scraping*. https://www.businesslive.co.za/fm/money-and-investing/2021-03-03-native-e-commerce-and-the-dangerous-rise-of-screen-scraping/

Google. (2021). *Google Safe Browsing*. https://transparencyreport.google.com/safe-browsing/overview

GOVERNANCE & STANDARDS DIVISION. (2017). *IT Risk Management Framework DOCUMENT REVISION HISTORY*.

Greene, M. (2019). *The password reuse problem is a ticking time bomb*. https://www.helpnetsecurity.com/2019/11/12/password-reuse-problem/

Grimes, A. R. (2020). *9 types of malware and how to recognize them*. https://www.csoonline.com/article/2615925/security-your-quick-guide-to-malware-types.html

Hope, A. (2021). *Almost All Organisations Suffered At Least One Data Breach in Past 18 Months, The State of Cloud Security Report Found*. https://www.cpomagazine.com/cyber-security/almost-all-organisations-suffered-at-least-one-data-breach-in-past-18-months-the-state-of-cloud-security-report-found/

Institute of Electrical and Electronics Engineers. (2014). *2014 Iranian Conference on Intelligent Systems (ICIS) : Higher Education Complex of Bam, Bam, Iran, 4-6 February [2014]*.

Irwin, L. (2020). *The 6 most common ways data breaches occur*. https://www.itgovernance.eu/blog/en/the-6-most-common-ways-data-breaches-occur

Johnson, D. (2020). *How often you should change your passwords, according to cybersecurity experts*. https://www.businessinsider.co.za/how-often-should-i-change-my-password?r=US&IR=T

Kaspersky. (n.d.). *What is Smishing and How to Defend Against it?* Retrieved August 25, 2021, from https://www.kaspersky.co.za/resource-center/threats/what-is-smishing-and-how-to-defend-against-it

Kaspersky. (2020). *The Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within*. https://www.kaspersky.com/blog/the-human-factor-in-it-security/

Kazmeyer, M. (n.d.). *Consequences for Companies Not Having Virus Protection*. Retrieved August 8, 2021, from https://smallbusiness.chron.com/consequences-companies-not-having-virus-protection-59157.html

Kure, H. I., Islam, S., & Razzaque, M. A. (2018). An integrated cyber security risk management approach for a cyber-physical system. *Applied Sciences (Switzerland)*, *8*(6). https://doi.org/10.3390/app8060898

Lazic, M. (2021). *41 Shocking Scam Statistics to Keep You Safe in 2021*. https://legaljobs.io/blog/scam-statistics/

Legezo, D. (2016). *Research on unsecured Wi-Fi networks across the world*. https://securelist.com/research-on-unsecured-wi-fi-networks-across-the-world/76733/

Liang, H., Peng, Z., Xue, Y., Guo, X., & Wang, N. (2015). Employees' exploration of complex systems: An integrative view. *Journal of Management Information Systems*, *32*(1), 322–357. https://doi.org/10.1080/07421222.2015.1029402

Limba, T., Plėta, T., Agafonov, K., & Damkus, M. (2017). Cyber security management model for critical infrastructure. *Entrepreneurship and Sustainability Issues*, *4*(4), 559–573. https://doi.org/10.9770/jesi.2017.4.4(12)

Luciano, E. M. (2014). *Influence of human factors on information security breaches-Luciano-Mahmood-Maçada*. https://www.researchgate.net/publication/260012210

Maalem Lahcen, R. A., Caulkins, B., Mohapatra, R., & Kumar, M. (2020). Review and insight on the behavioral aspects of cybersecurity. In *Cybersecurity* (Vol. 3, Issue 1). Springer Science and Business Media B.V. https://doi.org/10.1186/s42400-020-00050-w

Mcanyana, W., Brindley, C., & Seedat, Y. (2020). *INSIGHT INTO THE CYBERTHREAT LANDSCAPE IN SOUTH AFRICA*.

McKinsey & Company. (2017). *THE FUTURE OF RISK MANAGEMENT IN THE DIGITAL ERA*.

Model, A. I., Goel, R., Haddow, J., & Kumar, A. (2018). *Managing Cybersecurity Risk in Government: Managing Cybersecurity Risk in Government: An Implementation Model*. www.businessofgovernment.org

Mohammed, D., & Mohammed, S. (2017). Survey of Information Security Risk Management Models. In *International Journal of Business* (Vol. 7, Issue 4). www.ijbhtnet.com

Nobles, C. (2018). Botching Human Factors in Cybersecurity in Business Organizations. *HOLISTICA – Journal of Business and Public Administration*, *9*(3), 71–88. https://doi.org/10.2478/hjbpa-2018-0024

Norton. (n.d.). *Malvertising: What is it and how to avoid it*. Retrieved August 20, 2021, from https://us.norton.com/internetsecurity-malware-malvertising.html?om_sem_cid=hho_sem_sy:za:ggl:nt:d:br:kw0000692426:527805447241:c:google:181963234:108664493203:dsa-

403541485605&nortoncountry=ZA&gclid=CjwKCAjwiLGGBhAqEiwAgq3q_p6I9hYHUxhUixcwHgINSJd_Vn9XWHef_jhFkJ0-l6JmoyCBvgWjiBoCFiAQAvD_BwE&gclsrc=aw.ds

NRECA. (2011). *NRECA / Cooperative Research Network Smart Grid Demonstration Project Guide to Developing a Cyber Security and Risk Mitigation Plan*.

Nurse, J. R. C. (2019). Cybercrime and You: How Criminals Attack and the Human Factors That They Seek to Exploit. In *The Oxford Handbook of Cyberpsychology* (pp. 662–690). Oxford University Press. https://doi.org/10.1093/oxfordhb/9780198812746.013.35

O'Flaherty, K. (2019). *Top security risks in digital transformation – and how to overcome them*. https://www.information-age.com/security-risks-in-digital-transformation-123478326/

PandaSecurity. (2021). *The risks of using personal social media at work*. https://www.pandasecurity.com/en/mediacenter/tips/risks-social-media-work/

Parsons, K., Mccormac, A., Butavicius, M., & Ferguson, L. (2010). *Human Factors and Information Security: Individual, Culture and Security Environment*.

Patel, S., & Zaveri, J. (2010). A risk-assessment model for cyber attacks on information systems. *Journal of Computers*, *5*(3), 352–359. https://doi.org/10.4304/jcp.5.3.352-359

PPC Protect. (2021). *The Ultimate List of Click Fraud & Ad Fraud Statistics 2021*. https://ppcprotect.com/statistics/ad-fraud-statistics/

Redmiles, E. (2017). *Why Installing Software Updates Makes Us WannaCry*. https://www.scientificamerican.com/article/why-installing-software-updates-makes-us-wannacry/

Richter, F. (2020). *"Urgent Invoice" - How to Spot Malicious Emails*. https://www.statista.com/chart/17163/malicious-email-content/

RSA. (2020). *MANAGING DIGITAL RISK: 8 TYPES OF DIGITAL RISK AND HOW TO MANAGE THEM | MANAGING DIGITAL RISK 8 Types of Digital Risk and How to Manage Them*.

SCAMWATCH. (2021). *Scam statistics*. https://www.scamwatch.gov.au/scam-statistics

Sectigo. (2020). *Can I Get Malware Simply by Visiting a Website?* https://sectigo.com/resource-library/can-i-get-malware-simply-by-visiting-a-website

Shaw, R. S., Chen, C. C., Harris, A. L., & Huang, H. J. (2009). The impact of information richness on information security awareness training effectiveness. *Computers and Education*, *52*(1), 92–100. https://doi.org/10.1016/j.compedu.2008.06.011

Sophos. (2020). *THE STATE OF RANSOMWARE 2020*.

Spacey, J. (2015). *What is Organisational Risk?* https://simplicable.com/new/organizational-risk

SPAM LAWS. (n.d.). *The Danger of Pop-ups*. Retrieved August 20, 2021, from https://www.spamlaws.com/popup-dangers.html

st. Clair, A. (n.d.). *Sharing Passwords Hurts Your Business—Do This Instead*. Retrieved August 24, 2021, from https://www.teamoutpost.com/blog/sharing-passwords-hurts-your-business/

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers and Security*, *24*(2), 124–133. https://doi.org/10.1016/j.cose.2004.07.001

Statista. (2020). *Most common delivery methods and cybersecurity vulnerabilities causing ransomware infections according to MSPs worldwide as of 2020*. https://www.statista.com/statistics/700965/leading-cause-of-ransomware-infection/

Steinberg, S. (2019). *Cyberattacks now cost companies $200,000 on average, putting many out of business*. https://www.cnbc.com/2019/10/13/cyberattacks-cost-small-companies-200k-putting-many-out-of-business.html

Swinhoe, D. (2019). *What is a man-in-the-middle attack? How MitM attacks work and how to prevent them*. https://www.csoonline.com/article/3340117/what-is-a-man-in-the-middle-attack-how-mitm-attacks-work-and-how-to-prevent-them.html

TESSIAN. (2020a). *How to Identify a Malicious Website*. https://www.tessian.com/blog/how-to-identify-a-malicious-website/

TESSIAN. (2020b). *You Sent an Email to the Wrong Person. Now What?* https://www.tessian.com/blog/consequences-of-sending-email-to-the-wrong-person/

TESSIAN. (2021). *Understand the mistakes that compromise your company's security*. https://www.tessian.com/research/the-psychology-of-human-error/

The Hacker News. (2021). *Why Human Error is #1 Cyber Security Threat to Businesses in 2021*. https://thehackernews.com/2021/02/why-human-error-is-1-cyber-security.html

ThreatModeler. (2019). *Differences Explained: Threat vs. Vulnerability vs. Risk*. https://threatmodeler.com/differences-explained-threat-vs-vulnerability-vs-risk/

Tungal, A. T. (2021). *What is a Vulnerability?* https://www.upguard.com/blog/vulnerability#:~:text=In%20cyber%20security%2C%20a%20vulnerability,destroy%20or%20modify%20sensitive%20data.

Tungall, A. T. (2021). *How to Perform a Cyber Security Risk Assessment*. https://www.upguard.com/blog/cyber-security-risk-assessment

Wawrzyniak, D. (2006). *LNCS 4083 - Information Security Risk Assessment Model for Risk Management*.

Western Governers University. (2020). *What is the behavioral learning theory?* https://www.plutora.com/blog/digital-risk