Information system security vulnerabilities: Implications for South African financial firms in Cape Town

by

Sinoxolo Sisanda Hermanus

(Student No: 3564354)

Research report submitted in partial fulfilment of the requirements for the

degree of Master of Commerce Information Management

in the

Department of Information Systems

Faculty of Economic and Management Sciences

at the

University of the Western Cape

Supervisor Prof. Joel Chigada

November 2023

Acknowledgements

First and foremost, I thank God for blessing me with the opportunity to achieve my goals and complete this thesis. I could not have undertaken this journey without my late father's belief on the importance of education and encouragement for me to be better.

I would like to express my sincere gratitude to my supervisor, Prof. Joel Chigada, for his invaluable guidance and support throughout the completion of my study. Your expertise, support and patience helped me to complete this research and write this thesis.

I would like to express my gratitude to my mom, Nomzi Hermanus, my siblings and friends for the love and support throughout this journey. I wouldn't have been able to finish this adventure without your encouragement and motivation.

I would like to also thank my beloved daughter, Ncumolwethu Hermanus, for motivating me to strive for excellence.

Finally, I want to express my profound gratitude to all of the participants who took part in my research. Their willingness to share their experiences and insights has been extremely helpful to my research and has contributed to the success of this thesis. Thank you for your time and contribution.

PLAGIARISM DECLARATION

I, Sinoxolo Sisanda Hermanus, hereby declare that **"Information system security vulnerabilities: Implications for South African financial firms in Cape Town"** is my own original work and that all sources have been accurately reported and acknowledged, and that this document has not previously in its entirety or in part been submitted at any university to obtain an academic qualification.

Full name: Sinoxolo Sisanda Hermanus **Date:** November 2023

Signature:

ABSTRACT

Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the cyber environment and organisation and user's assets. According to the Utica University (2020) the rate of cybercrimes has grown exponentially and is consistent with the growth of technology. Additionally, due to the global Corona Virus Disease-2019 (COVID-19) pandemic, the cybercrime rate rose exponentially; The Interpol (2023) states that with organisations and businesses rapidly deploying remote systems and networks to support staff working from home, criminals are also taking advantage of increased security vulnerabilities to steal data, generate profits and cause disruption. Cybersecurity has become significant nationally, not only within companies, but also within societies.

This study analysed the factors that contribute to information systems security vulnerabilities in South African financial institutions; with the focus to addressing areas such as cybercrime, investments in cybersecurity and challenges, as well as the preparedness of organisations to address cybercrime. The study adopted an interpretivist approach, hence the use of a qualitative methodology. Microsoft Teams-based interviews were used to collect data from financial institutions' participants; these were recorded and analysed using thematic analysis method.

Findings revealed that the adoption of technologies in firms introduces cybersecurity risks and with technology advancements, new risks emerge; identified threats to organisations include third-party technologies and humans in the organisation. Participants mentioned phishing, insider attacks, and Distributed Denial of Service (DDoS) attacks that are usually experienced in organisations. Moreover, the study found that knowing your assets, frameworks, standards, and protection of Open Systems Interconnection (OSI) layers as strategies that financial firms adopt. Other strategies firms can implement include Identity and Access Management (IAM), data protection, detection systems, containment capabilities and incident response readiness, and cybersecurity training. However, the findings revealed that companies face challenges when implementing the strategies; these include business buy-in, availability, budget, skills, resources, regulatory compliance, building playbooks, and effective use of technologies. Even though the companies have adopted strategies, there is improvement needed. Lastly, the study offers recommendations to improve information systems security controls in order to reduce information systems security vulnerabilities.

Keywords: Cybersecurity, cybercrime, South African financial firms, information systems security vulnerabilities.

Table of Contents

LIST OF FIGURES

LIST OF TABLES

LIST OF ACRONYMS

AI	Artificial Intelligence
APT	Advanced Persistent Threat
API	Application Programming Interface
ASV	Approved Scanning Vendor
ATMs	Automated Teller Machines
BYOD	Bringing-Your-Own-Device
CMMI	Capability Maturity Model Integration
CSIS	Center for Strategic and International Studies
XSS	Cross-Site Scripting
CIA	Confidentiality, Integrity, and Availability
CII	Critical Information Infrastructure
CIS	Critical Security Controls
COBIT	Control Objectives for Information and Related Technologies
CPM	COBIT performance management
DMZ	Demilitarised Zone
DDoS	Distributed Denial-of-Service
DoS	Denial of Service
ECT	Electronic Communications and Transactions
GDPR	General Data Protection Regulation
HIPAA	Health Insurance Portability and Accountability Act of 1996
IAM	Identity and Access Management
ICT	Information and Communication Technologies
IDS	Intrusion Detection Systems
IOCs	Indications of compromise
IoT	Internet of Things
ISACA	Information Systems Audit and Control Association
ISO/IEC	Information Security Management 27001
ISMS	Information Security Management System
ITIL	Information Technology Infrastructure Library

M2M	Machine-to-Machine
MitM	Man-in-the-Middle
MFA	Multi-factor authentication
ML	Machine learning
NCPF	National Cybersecurity Policy Framework
NIS	Network and Information Systems
NIST	National Institute of Standards and Technology
OTA	Over-The-Air
PASA	Payment Association of South Africa
PCI	Payment Card Industry
PCI DSS	Payment Card Industry Data Security Standard
PIN	Personal Identification Number
PBRM	Plan, Build, Run, and Monitor Responsibility areas
POPIA	Protection of Personal Information Act
PRM	Process Refence Model
RBAC	Role-Based Access Control
SAD	Sensitive Authentication Data
SAFPS	Southern African Fraud Prevention Service
SVS	Service Value System
SIEM	Security Information and Event Management
TOGAF	The Open Group Architecture Framework
UEBA	User and Entity Behaviour Analysis
URL	Uniform Resource Locator
XXE	XML External Entities

CHAPTER 1
INTRODUCTION AND BACKGROUND

1.1 Introduction

There has been an exponential rise in cybercrimes globally, specifically targeting healthcare, financial and government institutions in the period where the global Corona Virus Disease2019 (COVID-19) pandemic emerged in 2019 (World Health Organisation, 2020). Many people and firms are relying on information and communication technologies (ICTs). Nyasvisvo and Chigada (2023) mention that the global outbreak of the respiratory COVID-19 in 2019 claimed many live and altered the way most people lived and behaved, which made it necessary to reconfigure business models. Zerlang (2022) adds that the Covid-19 outbreak prompted businesses around the world to rapidly shutter their offices to minimise the spread of disease, kick-starting the overnight migration to a remote work force. However, Zerlang (2022) points out that expanding work beyond the office also resulted in an expansion of businesses' network perimeters, opening up new, widely-spread vulnerabilities which threat actors have pounced on. The most vulnerable industries to cyberattacks, according to Alawida, *et al.* (2022), were healthcare and banking industries.

Chigada and Madzinga (2021) argue that cyberattacks and threats against financial institutions rose by more than 238% globally between February and April 2020, at a time when the global economy was working tirelessly to combat COVID-19 infections. In addition, the demand for company and personal information assets is driving the rise in cybercrimes, resulting in organisations losing huge sums of money. Van Niekerk (2017) states that even though cybersecurity issues are rising globally, fuelled by allegations of ever-larger data breaches and a shortage of trained cybersecurity professionals; most organisations and nations seem to be failing to come up with interventions to respond effectively. In South Africa, Van Niekerk (2017) argues that cybersecurity is hitting a critical point just like in other countries, hence the significance to find the resolutions to the problem at hand for South Africans to be able to protect themselves from cyber criminals. However, GoJ (2015) argues that it is necessary to ensure multi-layered cybersecurity for the realisation of a society in which citizens can live safely and securely, through the cooperation of multi-stakeholders, including government bodies, local governments, cyber-related businesses, critical infrastructure operators, educational and research institutions, and every individual. Despite the existence of multi-layered approaches, cybercriminals are well-versed with trends and in most instances are a step ahead in their nefarious actions.

The International Information System Security Certification Consortium [ISC] 2 (2019) states that companies can use a strategy of either building a strong cybersecurity team from inside the company or outside the company. Building from inside the organisation occurs when the firm wants to keep up with its inhouse professionals in place to help them to build the skills and expertise that are continually improving to protect their organisations in the future. In addition, building from outside the company means firms attempt to employ people with appropriate and thorough work experience, advanced knowledge of principles, and certificates for cybersecurity. In addition, Gcaza and von Solms (2017) and Chigada (2023) state that the proposed national cybersecurity culture strategy of companies should take into consideration gaps such as increased government accountability, lack of resources, poor stakeholder management, lack of regulation, skilled human resources, research and development, and lack of monitoring and evaluation when formulating the strategy.

1.2 Background of study

The InfoSec Insights (2021) defines cybersecurity as the process of protecting the technologies and data against cybersecurity threats and attacks — many of which lead to costly cybercrimes. With an ever-changing digital landscape, the cyberattacks change due to the evolving targets, evolving impact, and evolving techniques (Accenture Security, 2019). There are new devices and technologies which are increasingly being developed and becoming more accessible to consumers. Firms need to always keep track of the latest trends of cyber threats and attacks to stay consistent in securing their systems. Additionally, a high number of technical security controls are used by many organisations, but they still show a non-proportional number of security breaches; this occurs because information security is primarily an unaddressed human factor issue (Safianu, Twum, and HayfronAcquah, 2016). This means that investing in users is as important as investing in technology, as mostly these systems are used by individuals/employees to perform the tasks of the organisation. Cybersecurity breaches are a basic problem to private firms, public firms and, to individuals. Research shows that the most pervasive malicious attacks in 2020 were on consumer, employee and corporate data, accounting for 48% of incidents, and proving to be the costliest cause of business breaches (Dlamini, 2020).

South African financial organisations, just like in many other countries, are gradually adopting digital transformation strategies to stay competitive in the modern digital economy. South Africa

has recognised the need to encourage digital promotion, more strongly in organisations by increasing awareness of the value of Information and Communications Technology for inclusive economic development (Innovation, 2019). Technological advancements are creating opportunities for cybercriminals to illegally access, modify, steal, and disrupt information systems. Accenture Security (2019) states that as the world become increasingly connected and technology more sophisticated, the threat landscape becomes more complex and potentially damaging. This means that as organisations adapt to the use of new technologies, the more likely it is for cybercriminals to access, modify, steal, and disrupt their systems illegally. South Africa is faced with challenges such as lack of investment in cybersecurity, developing cybercrime legislation and law enforcement training, and poor public knowledge of cyber threats (Mcanyana *et al*., 2020).

1.3 Statement of research problem

The lack of cybersecurity investment to reskill human resources, absence of information systems security strategies and lack of awareness to employees, place financial institutions in vulnerable positions. Africa (2020) states that the lack of preparedness for cybersecurity continues to generate issues and threats for South African businesses as in the recent improvements in the way people operate have created a multitude of ways for cyber criminals to manipulate vulnerabilities in systems, procedures, and behaviour. As people work from home due to the COVID-19 pandemic, they become more exposed to the cyber criminals as some companies do not put in security measures for devices and public networks that employees use in their daily activities. Home-based work increases exposure to cyber-risks because individuals connect through less reliable and unsecured Internet connections (Chigada and Madzinga, 2021). This makes it easy for threat actors to attack the company systems through illegal activities. For example, Moyo (2020) states that the attack against Nedbank occurred through the third-party service provider, which issues Short Message Service (SMS) and e-mail marketing information on behalf of the bank and several other companies. Also, Osborne (2020) states that Amalgamated Banks of South Africa (Absa) identified an isolated internal data leak whereby personal information of a limited number of Absa customers was shared with parties external to the bank. Financial institutions are needed to develop and implement good cybersecurity strategies to prevent such events occurring in the near future. Africa (2020) mentions that most Information Technology (IT) teams have been concentrating on empowering staff rapidly to function remotely and to ensure continued business activities, forcing on the backburner of network security.

Internet users in South Africa are inexperienced and less technically skilled compared to users in other countries (Mcanyana *et al.*, 2020); this makes users more vulnerable to the cyberattacks . With the increasing number of internet users, the more the exposure to cyber criminals. Through the use of smartphones, and other electric devices, as most services of companies are accessed online, companies are likely to be attacked as most individuals are not educated enough on Information Systems Security. The IT-Online (2013) states that there is a rise of mobile device exploits; companies are experiencing an increase in the number of exploits on mobile devices (especially smartphones) which increases the security risk profile of allowing such devices to connect to the corporate network. These issues need to be addressed urgently as the country is always adopting new technological advancements.

South Africa's primary challenge is the long process of developing and enforcing strategies and processes to tackle cybercrime (Dlamini and Mbambo, 2019). The common law is unable to solve the cybercrime as cybercrime deals with intangibles. Chigada and Kyobe (2018) argue that in South Africa, the current shared legal arrangements are based on formal, complex, time-consuming, and difficult to understand procedures that result in misalignment and non-compliance with e-legislation.

1.4 Primary research question and sub-questions

1.4.1 Research question

What factors contribute to information systems security vulnerabilities in South African financial institutions?

1.4.2 Sub-questions

The following sub-questions were developed and served as a roadmap for data collection of this study.

- What is the current state of cybercrimes in South African financial sector?
- To what extent do South African financial institutions invest in information systems security?
- What challenges are faced by South African financial institutions when implementing cybersecurity strategies?
- How prepared are the financial institutions to address cybercrimes?

- How can firms improve their information systems security controls in order to reduce information systems security vulnerabilities?

1.5 Research objectives

- To evaluate the level of cybercrimes in the South African financial sector.
- To examine the level of South African financial firms' investments towards the information systems security.
- To evaluate the state of readiness of financial institutions to address cybercrimes.
- To identify challenges that are encountered by South African financial institutions when implementing cybersecurity strategies.
- To gather recommendations and solutions on how financial firms can improve information systems security controls to reduce cybersecurity vulnerabilities.

1.6 Location of the study

This study was conducted in the financial firms around the Cape Metro, Western Cape. The researcher resides in the Western Cape and those financial firms were much more accessible compared to the firms in other provinces. Additionally, financial firms in the area also have branches in other provinces of South Africa, which can helped bring out a broader view on the implications of Information system security vulnerabilities South African financial firms in general.

1.7 Contribution of the study

The researcher clearly outlines the benefits of the study for society at large and in particular for people, corporate entities, the government and/or its agencies, as well as explains the study's possible contributions to the body of knowledge in a particular subject or field (Adu and Badaru, 2022). The contributions of this study are discussed below.

1.7.1 Methodological Contribution

The methodological contribution of this study is the experience obtained with adopting an exploratory approach and the methods used for data collecting constitutes which might be beneficial to other research on the vulnerabilities implications of information systems security in financial firms.

1.7.2 Practical contribution

The data collected from this study provides detailed insights on the information systems security vulnerabilities of South African financial firms in Cape Town. The data includes providing an understanding of the adoption of cybersecurity and its investment by the financial firms, security issues in these firms, and ways in which can be used to combat those issues. Through this study, financial institutions are assessed for their readiness to address cybercrimes for better security in firms. The findings of the study can assist financial institutions and other industries plan, address cyberattacks and improve their security posture to protect against cyber threats. Moreover, recommendations provided in this study can be advantageous to financial institutions if they adopt and implement them.

1.7.3 Theoretical contribution

As South Africa is faced with a lot of challenges and is behind with the technology adoption; the aim of the study was to find ways to improve the information systems security and lower its vulnerabilities for the greater good of the economy as this thesis will not only be accessible to Cape Town firms but the society as a whole. Furthermore, this study is of significance as it provides an opportunity for policy makers to review the current cybersecurity policies in South Africa and improve those. The study explores and provides the future possibilities of information systems security for institutions to stay prepared.

1.8 Thesis outline

The thesis consists of six chapters presented below.

1.8.1 Chapter 1: Introduction and background

This chapter presents the introduction and background of the research study. It briefly describes the background of the study, research problem, research questions and subquestions, research objectives, location of the study and importance of the study.

1.8.2 Chapter 2: Literature review

This chapter explores the existing literature on information systems security in South Africa and other countries as well as other related themes. The chapter begins with an introduction then followed the discussion of cybercrime globally and in South Africa. Additionally, the chapter outlines the topologies of cybercrime and their impact on the economy. Further, the

chapter provides the discussion of the South African cybersecurity landscape, cybersecurity globally and in South Africa, and the summary of the chapter.

1.8.3 Chapter 3: Information security standards

This chapter presents information security standards relating to financial firms. The chapter begins with the introduction then discusses the themes: Information Security Management (ISO/IEC) 2700, National Institute of Standards and Technology (NIST), Control Objectives for Information and Related Technologies (COBIT), Information Technology Infrastructure Library (ITIL), Payment Card Industry Data Security Standard (PCI DSS), Center for Internet Security (CIS) Critical Security Controls, and summarised information security standards.
Lastly, the chapter provides the concluding remarks.

1.8.4 Chapter 4: Research design and methodology

This chapter focuses presenting the research design and methodology used in the study for data collection. The chapter begins with an introduction, followed by the discussion of the research paradigm, research design, research method, target population, instrument development, sampling techniques, and pilot study. Moreover, the chapter outlines the data analysis, trustworthiness of the study, and ethical considerations. Lastly, presents the concluding remarks.

1.8.5 Chapter 5: Findings and results discussions

This chapter provides the detailed findings and results of data collected from the financial firms through sampled participants. The results are presented in relation to the analysis of the literature conducted in an effort to address the research questions as well as the theoretical framework that underpins this study.

1.8.6 Chapter 6: Conclusion and recommendations

This chapter provides a conclusion to the whole study and recommendations to financial institutions on how they can improve information systems security controls with the aim to have effective strategies and reduce cybersecurity risks.

1.9 Chapter summary

In this chapter the introduction and background of the study were discussed. It further presented the research question and sub-questions, research objectives, location of the study,

importance of the study, and the outline of the whole thesis. The next chapter reviews literature pertaining to cybersecurity, information security and cybercrime.

CHAPTER 2
LITERATURE REVIEW

2.1 Introduction

In this chapter, the researcher reviews the literature on cybersecurity in South Africa to provide factors that influence the challenges South African companies face in preventing cybercrime. The literature review begins by describing an overview of cybercrime, firstly globally and then in South Africa. The second discussion of the chapter is about the types of cybercrime and their impact on the economy. Moreover, the chapter discusses the cybersecurity landscape in South Africa and lastly, the interventions to mitigate cybercrime (which is cybersecurity).

2.2 Overview of cybercrime

Allen (2021) states that cybercrime includes, but is not limited to, unauthorised access to a computer or device such as a universal serial bus (USB) drive or an external hard disk; illegal data interception; unlawful password acquisition, possession, receipt, or usage; and online forgery, fraud, and extortion. Thomas (2020) defines cybercrime or cyberheist as any malpractice associated with interactions on the internet, including theft of data and identity, financial scams, and security threats. Similarly, Chigada (2021) defines cybercrime as any unlawful activity perpetrated by a criminal through Internet-based transactions with the intention of destroying, inflicting emotional, psychological harm, financial loss and reputational damage to a person of organisation. Lazic (2023) mentions that the internet statistics show that hackers attack people worldwide roughly every half a minute, which translates to a cybercrime being committed on an average of 2,244 times per day.

Over the years, there has been significant growth in cyberattacks , which makes cybersecurity an interesting site for research, where organisation can find ways to prevent these attacks.

Cyberattacks have been rated the fifth top rated risk in 2020 and become the new norm across public and private sectors, and the risky industry continues to grow in 2023 as Internet of Things (IoT) cyberattacks alone are expected to double by 2025 (McLean, 2023). Compared to 2021, Anderson (2023) states that new data on cyberattack trends cites a 38% increase in global attacks in 2022. Recent security research suggests that most companies have poor cybersecurity practices in place, making them vulnerable to data loss (Sobers, 2021). As a result, Huang *et al.* (2023) argue that that cyber risks are skyrocketing; the IBM data breach report revealed that an alarming 83% of organisations experienced more than one data breach during 2022. Cyber actors routinely exploit poor security configurations (either misconfigured or left unsecured), weak controls, and other poor cyber hygiene practices to gain initial access or as part of other tactics to compromise a victim's system (Cybersecurity and Infrastructure Security Agency, 2022). Furthermore, the increase in the percentage of people connected to the internet and the amount of time spent online. This, coupled with the sensation of confinement and anxiety and panic caused by the lockdown, has given cybercriminals more significant opportunity to profit from the situation or cause disruption (Radoini, 2020).

2.2.1 Cybercrime in South Africa

It is known through Goodman *et al.* (2015)'s work that the advanced infrastructure in South Africa is being used as a base for regional cybercrime activities. Cybercriminals are becoming more agile, leveraging new technology at lightning speed, customising their attacks with novel approaches, and collaborating in ways we have never seen before (Darknet, 2021). With new technology advancements, there is more growth in cybercrime. This is despite a new wave and complex strategies used by cybercriminals which are more advanced than the contemporary enterprise's information security strategy. One explanation for the growth in cybercrimes despite efforts made is that *"South African firms are still using old and irrelevant solutions to combat, address and mitigate cybercrime.* ", (Chigada, 2021).

Another explanation can be found in Allison (2022)'s study when he states that as technology advances, so do hackers' abilities to identify weaknesses and flaws in organisations' security protocols. This according to Allison (2022) creates a serious cybersecurity issue because the hackers are able to access the protected data and files. The exploitation of vulnerabilities in South Africa was also brought to attention noting that the country has the third-highest global victimisation rate of cybercrime which costs R2.2 billion annually (Kavanagh and Sharif, 2021).

Consequently, the following significant attacks in South Africa are listed in Mcanyana *et al*. (2020): in the first quarter of 2019, malware attacks in South Africa rose by 22%, relative to the

first quarter of 2018, which corresponds to just under 577 attempted attacks per hour. Additionally, in South Africa, Android mobile phones were the second most targeted by malware for banking. Malware detections rose by 8% in the first quarter of 2019 compared to the same period in 2018, with mobile malware increasing by over 17%, far more than computer malware. There was an increase in virtual-currency-related crime,3 with hackers increasingly using individuals' phones to mine cryptocurrencies. Card-not-present (CNP) fraud on credit cards issued by South Africa remained the country's leading contributor to gross fraud losses, accounting for 79.5% of all losses. Lastly, South Africa has seen a more than 100% rise in smartphone fraud of banking applications.

Pinnock (2020) states that the COVID-19 pandemic seemed to be escalating the rate of attacks, as a result within the first 100 days of the pandemic in 2020, a Mimecast Threat Intel study found a 75% rise impersonation fraud in South Africa. Such results show that the rise in technological advancements leads to greater vulnerability to cyber threats and attacks. Collard (2021) argues that in the coming year, attacks such as phishing emails, criminals might start applying artificial intelligence (AI) and emerging technology in their social engineering attacks, cloud jacking attacks and ransomware are expected to rise. Barlow (2023) points out that the rapid transition to remote work culture has increased exposure, creating a breeding ground for cyberattacks to take place both in and outside the office, and against both personal and business devices. As employees are working remotely it is in the best interest for organisations to invest in information systems security to prevent attacks through employee devices.

Financial institutions are among the six most targeted industries for cyberattacks (Manship, 2022). The financial organisations hold many financial data that can be used to commit fraud or theft. According to Subhani (2023) financial institution's servers host data files that contain sensitive information, such as users' personal and financial information; this information is highly appreciated on the dark web. Additionally, Mottl (2022) argues that customers' lives have been made easier by cloud applications, but end-to-end security is now more difficult, which means that if a hacker gains access to the system, there is a risk of data loss, exploitation, and business interruptions.

The South African Banking Risks Information Centre [SABRIC] (2023) states that cybercrime is an increasing socio-technical problem at an alarming rate and will soon replace many 'traditional' banks crimes due to its virtual nature, which allows it to transcend time and physical proximity. Additionally, Hasham, Joshi and Mikkelsen (2019) suggest that the vulnerabilities to fraud and financial crime inherent in automation and digitisation, tremendous growth in

transaction volumes, and growing integration of financial systems within countries and globally are all risks for banks. The magnetic stripe, which is present on bank-issued cards in South Africa that holds sensitive card and cardholder data (person's card number, card's expiry dates and other unique identifiers), is easily exploited by criminals like the as (Chigada, 2020).

Cyberattacks on businesses across Africa are increasing at an alarming rate, making cybersecurity a crucial priority for businesses (Jackson, 2023). Attackers target external assets and software that are not visible to security practitioners that rely on conventional attack surface management and vulnerability management solutions alone; to reduce cyber risk and bridge the IT security gap, the modern enterprise must be able to achieve complete visibility of both internal and external internet-facing assets (Qualys, Inc., 2023). Many companies have been attacked including the highly sophisticated attack to RSAWEB in 2023 which resulted in services going offline, Transnet in 2021 had an extreme downtime and disruption followed a ransomware attack, a major ransomware hit on City Power, and many more. As a result of the mentioned above attacks, City Power prepaid consumers were unable to buy electricity units. Secondly, the Transnet attack affected the country's port and container terminal operations as, as result, a number of ships and trucks were left idling. If strict measures are not taken to counteract this alarming trend of card fraud including debit card fraud, it is anticipated that it will persist. Koigi (2020) states that cyber threat actors' increased interest on South Africa is due to linked factors such as lack of cybersecurity investment, the growth of cybercrime laws and law enforcement training, limited public awareness of cyber threats, to name a few. Additionally, the research by Koigi (2020) reveals that this results from issues that South Africa has been experiencing for years, and there is still no way forward. Laubscher (2018) argues that the South African economy is faced with a number of obstacles, including political instability that may deter investment, a high unemployment rate, inflation, crime, a trade imbalance, a volatile exchange rate, and one of the biggest obstacles is a lack of skills. Moreover, NCPF (2015) states that South African vital data infrastructure continues to be vulnerable to some degree as the country is an ICT consumer and relies on technology manufactured abroad to protect its cyberspace; this means that the lack of development of cybersecurity technologies is adding to the problems that the country face. Furthermore, there is a need to build an enabling environment for South Africa's cybersecurity training, education, Research and development, and skills development programmes (NCPF, 2015). These programmes include raising awareness among the public about safe measures on the internet, conducting research on the latest cybersecurity affairs that will impact the people and companies, and providing cybersecurity technical skills.

Budnik and Kirkwood (2021) argue that financial firms need improved cooperation through cybersecurity, anti-fraud, and anti-money laundering controls, to develop a corporate governance model, and consider meeting counterparts in other financial crime pillars and initiating conversations around the concept of convergence to better understand risks and manage cybercrime. Furthermore, Utica University (2020) states that the frequency and sophistication of cybercrimes increase along with technological advancement, fortunately, as technology has developed, so too has the capacity to prevent cybercrimes from occurring and to defend people when they occur.

2.3 Topologies of cybercrime

The types of cybercrimes which pose the greatest information systems security risks are discussed below.

2.3.1 Internet of thing (IoT) attacks

Every second, 127 new gadgets connect to the internet; there are many IoT devices, and defending such a large attack surface is difficult, especially when the devices are of various types and security standards (Brooks, 2021). Organisations and people use IoT devices; with advances in technology and each device connected to the internet, vulnerabilities increase. Every device stands a chance of being attacked by criminals. Patel (2021) identifies inconsistent security standards, low processing power, legacy assets, lack of awareness of the users, botnet attacks, lack of encryption, firmware updates missing, and rogue and counterfeit IoT devices as the security threats and challenges for IoT devices and description of each is provided below:

i. Inconsistent security standards

The lack of standardisation makes it more challenging to protect IoT devices and allow machine-to-machine (M2M) communication without increasing security risks. Additionally, the lack of standardised security protocols means that IoT devices are often left vulnerable to cyberattacks and makes it challenging for developers and IT professionals who need to integrate multiple systems with varying levels of security into a cohesive network environment (Device Authority, 2024). Since there is no global standard for firms and niches, Patel (2021) argues that each company must set its own rules and guidelines.

ii. Low processing power

Henke (2023) states that most IoT apps require very little data, which makes over-the-air (OTA) updates difficult and prevents the device from using security features like firewalls, virus

scanners, and end-to-end encryption. According to the IT Pillars (2022), the burden falls to the network the devices are connecting to, hence there is a need for strong network security to protect against security attacks relating to lower processing power and all devices, including small devices need to be protected.

iii. Legacy assets

According to Topping (2024), updating and integrating legacy systems in an IoT ecosystem can pose detrimental security risks, as outdated systems and hardware are more vulnerable to a variety of sophisticated attacks that were not considered when these systems were in development. For example, if an app was not designed with cloud connectivity in mind, it is likely to be exposed to today's cyber threats; more contemporary encryption standards may not be compatible with certain older assets. There is a need for organisations to monitor, constantly update, securely provision for legacy systems and network vulnerabilities to ensure a tight security infrastructure (Topping, 2024).

iv. Lack of awareness of the users

Over the years, the number of technology users has increased, and more people connect to the internet. As the Internet of Things is a relatively new technology, Patel (2021) states that many people are unfamiliar with its concepts and capabilities, resulting in IoT devices representing major security concerns to manufacturers, consumers, and businesses. The Nexus Group (2024) further states that users who lack awareness of IoT security may overlook the importance of configuring devices securely, neglect firmware updates, and use weak passwords.

v. Botnet attacks

Botnets are frequently used to construct, automate, and speed up an attack at a minimal cost and in a short time. These devices are remotely controlled as a group without the owner knowing and hackers use botnets to carry out a range of malicious activities, including stealing data (Nexus Group, 2024). It may be difficult for security systems to distinguish between legitimate and malicious transmissions. vi. Lack of encryption.

With many IoT devices not encrypting the data they transmit, passwords and other sensitive information sent to and from the device can be intercepted if a network is breached. Ahatlan (2022) reveals that having a “man-in-the-middle” or MitM can be dangerous for IoT security; it happens when an IoT device will communicate in plain text. vii. Firmware updates Missing

Another considerable IoT security risk is if devices are released with a bug that causes security flaws. Manufacturers must upgrade their firmware to avoid these dangerous scenarios, whether from their code or code produced by a third party (Henke, 2023).

viii. Rogue and Counterfeit IoT devices

The tremendous rise in popularity and volume of production of Internet of Things devices has raised concerns about home networks. Users are unintentionally installing rogue and counterfeit IoT devices insecure networks; these devices either replace the originals or integrate into the network to gather essential data and information, thus breaching the network perimeter (Ganguly, 2023).

2.3.2 Cloud attacks

Robison (2021) argues that while businesses used to be expected to own and operate their data centres, by 2022, the percentage of business software running on traditional servers is likely to drop to 32% of all enterprise applications, approximately half of what it was in 2019. Companies have been adopting cloud methodologies to maintain competitive advantage; the number of cloud adopters increased more when the COVID-19 lockdown started. Because of the unpredictability of the times and the potential reality of the "new normal," an increasing number of businesses began to lay out their plans for cloud computing and digital transformation (Aggarwal, 2021). Hence the significance of cybersecurity in cloud computing. Al Mehdar (2020) states that the threat landscape is continuously changing; it is critical to minimise the risk of cloud computing and ensure that data and systems are secure at rest, in use, and in transit. Katrenko (2021) discusses the following as the critical cloud computing vulnerabilities that raise security concerns among cloud users;

i. Data threats

Due to human activities, application vulnerabilities, and unforeseen events, the many forms of data stored in the cloud are prone to lose, breach, or damage. Although no cloud service provider can prevent all data threats, cloud developers should employ modern encryption methods to ensure that data from the user to the cloud is secure.

ii. Cloud vulnerabilities

The vulnerabilities in application programming interfaces may substantially impact cloud orchestration, management, provisioning, and monitoring security. Kosten (2020) argues that developers create APIs without proper authentication controls; these are open to the internet, and anyone can use them to access enterprise data and systems. Moreover, too many developers do not think attackers will see backend API calls and don't put appropriate

authorization controls in place (Kosten, 2020). Studies show that threat actors can simply launch DDoS attacks and obtain access to sensitive company data by taking advantage of unsecure APIs while remaining unnoticed.

iii. Malicious insiders

Attacks or data leaks can be planned in cloud systems in various ways by legitimate cloud users. Insider threats misuse the authorised access to critical assets of the organisations for their malicious behaviour. The human element becomes increasingly more important as more businesses use cloud services; hence users of cloud services must be aware of the steps providers are taking to identify and stop the threat posed by harmful insiders (Mahajan and Sharma, 2015). iv. Shared technology vulnerabilities

Virtualisation and cloud orchestration are two examples of shared technology used in cloud computing. Attackers might cause severe damage to multiple cloud users by exploiting weaknesses in any element of shared technologies. Hackers can use flaws in a hypervisor to acquire control of virtual machines or even the host itself. Hackers can acquire full access to the host in a virtual machine escape by using shared resources.

v. Provider lock-in

When moving data, products, or services to a different vendor's platform is complex and costly, customers become more reliant (locked-in) on a single cloud storage provider. According to Friend (2022) one of the most pressing challenges of lock-in with hyperscalers is security concerns; storing all of your data in one place is equivalent to placing all your eggs in one basket when it comes to security and uptime. This means that an organisation bets that a malware attack will be unable to bypass the security of the provider, and that provider can provide 24/7 uptime (Friend, 2022).

vi. Weak cryptography

Cloud providers utilise cryptographic techniques to secure data in storage, however, they often rely on limited sources of unpredictability (such as time) to produce random numbers for data encryption. RSI Security (2019) states that the biggest issue is the security key. An example provided by RSI Security (2019) is that if the assigned password is lost during the process of encryption in the cloud, there is no way to salvage the data, and people create common words, such as their email passwords or spouse's name. Lastly, one of the cloud issues with encryption is the false sense of security which is created by its complex processes and procedures. (RSI Security, 2019). The author states that encryption is still not a perfect solution for data security, just like any other measures.

vii. Vulnerable cloud services

An attacker can take advantage of weaknesses in any cloud service to get unauthorised access to legitimate users' data. Kosten (2020) argues that insecure cloud storage buckets can result in attackers gaining access to data stored in the cloud and downloading confidential data, which can have devastating consequences for organisations. Further, Meharchandani (2021) states that one of the best ways for firms to stay ahead of threats is by conducting regular cloud penetration testing and mitigating all the detected vulnerabilities on priority.

2.3.3 Insider attacks

Imperva (2023) describes insider threats as a security risk involving a current or former employee or business associate who has access to sensitive information or privileged accounts within an organisation's network and who misuses this access. These attacks can result in significant financial and reputational damage to the company. Pritz (2021) states that it is predicted that insider data breaches will rise 8% in 2021 and that a third of all incidents will be caused internally. Many companies are wholly unprepared to deal with these kinds of threats. Further, as employees started to work from home due to the COVID-19 pandemic lockdown, the number of insider attacks increased. Rosenthal (2022) states a 47% increase in the number of incidents involving insider threats between 2018 and 2020; this encompasses intentional data exfiltration and data loss due to human error. For example, Malinga (2021) mentions that an employee at Absa leaked customer data and sold it to a small number of third parties for personal financial gain and the bank confirmed investigations into the data leak revealed a total of 209 000 customers were affected by the leak, which is approximately 2% of its total local client base.

2.3.4 Blockchain and cryptocurrency attacks

Upadhyay (2020) argues that the terms blockchain and cryptocurrency may be unfamiliar to the ordinary internet user but are extremely important to businesses. As a result, Upadhyay (2020) adds that attacks on these frameworks represent significant issues for organisations in terms of cybersecurity, as they might endanger client data and business processes. Organisations need to ensure that they are updated with risks relating to blockchain and cryptocurrency and find ways to prevent cybercriminals from attacking them. Seifried (2020) states that the Cloud Security Alliance has documented a preliminary list of around 200 issues related to blockchain and smart contracts, about half of which are not listed in any other public database of vulnerabilities.

2.3.5 Machine learning (ML) and artificial intelligence (AI) attacks

Malicious actors can use ML and AI technologies to carry out cyberattacks and these pose a threat to enterprises. These methods can find high-value targets in massive datasets. For example, Ciancaglini, Gibson, and Sancho (2020) argue that malware developers can use AI in more obfuscated ways without being detected by researchers and analysts, as a result, it is only possible to search for observable signs that might be expected from AI malware activity. Researchers, for instance, have been able to craft malware with features that allow it to remain undetected even by ML-based antivirus engines (Ciancaglini, Gibson, and Sancho, 2020). Additionally, AI and ML have become critical technologies in information security since they can quickly analyse millions of events and identify a wide range of threats, from malware exploiting zero-day vulnerabilities to detecting risky behaviour that could lead to a phishing attack or malicious code download (Balbix, Inc., 2023). As more businesses focus on largescale AI-powered digital transformations, those risks become more vulnerable. System manipulation, data corruption and poisoning, transfer learning attacks, online system manipulation, and data privacy are the top five security threats facing artificial intelligence and machine learning (Dror, 2021). Further, organisations need to use security solutions that provide highly protected confidential computing environments to secure their AI applications and machine learning models.

2.3.6 Hacking

Teimoor (2019) defines hacking as identifying weaknesses in computer systems or networks to exploit its weaknesses to gain access. For example, with recent incidents, Mabuza (2020) states that the SABRIC announced that the credit bureau Experian suffered a data breach, revealing the personal information of up to 24 million South Africans. Moreover, Smillie (2019) states that the Johannesburg local government and finance sector was hacked by two separate groups threatening to close them down when South Africans would pay municipal bills and gain access to their bank accounts. Furthermore, another group of hackers has threatened to leak customer details from the City of Joburg unless charged four Bitcoins.

2.3.7 Email bombing and spamming

Houle and Pandey (2018) describe email bombing as a form of Denial of Service (DoS) attack that consists of sending huge volumes of email to one or more email addresses to overflow the mailbox or overwhelm the server where the mailbox is hosted. This results in the victim's email account or mail servers crashing. Moreover, Domains.co.za reported that that they experienced a dramatic increase in SPAM attacks on the company's servers in 2020.

Fortunately, due to the company's multi-pronged proactive approach to malicious communications, this surge was identified early, introducing mitigation for it. BusinessTech (2016) also reported that the SABRIC introduced its Schemes and Scams Campaign, which aimed to raise awareness about banking scams in the country. In this report, the explanation was that the cybercriminals would send an email or letter informing the potential business victim that their supplier has changed their bank account details. The new fraudulent account information is included in the criminal's correspondence for the victims to pay.

2.3.8 Phishing

Deloitte (2019) states that phishing happens when an attacker pretends to be a trusted entity to swindle a victim into clicking a malicious connection, leading to a malware installation, device freezing as part of a ransomware attack, or exposing confidential information. As describes by Cisco Systems, Inc., (2023) *"A phishing attack relies on a social-engineering effort where hackers create a counterfeit communication that looks legitimate and appears to come from a trusted source. Attackers use seemingly benign emails or text messages to trick unsuspecting users into taking an action such as downloading malware, visiting an infected site, or divulging login credentials in order to steal money or data".* Unlike ransomware attacks, the hacker does not block confidential user data after obtaining its access. South Africa experienced a rise in phishing attacks during the COVID-19 national lockdown. Walker (2020) argues that as the pandemic progressed, there were three distinct ways of phishing attacks as follows;

i. Phishing attacks providing basic information about the pandemic, and spam/scam emails advertising dubious goods and services, were part of the first wave.
ii. The second wave introduced fresh, and novel phishes, with cybercriminals attempting new strategies to convince users to view malicious content. iii. The researchers have seen repurposed standard phishing models converted into corona-virus-related phishing scams in the third wave.

Moreover, businesstech.co.za (2021) states that in South African banks, the most common fraud of 2021 was phishing. For example, a person tries to trick a customer into giving them confidential information by pretending their email communication was sent from the bank. businesstech.co.za (2021) states that 59% of the South African internet-banking population was aware of it and 15% of the population reported being targeted, while 4% of them fell prey to it.

2.3.9 Vishing

Vishing's purpose is similar to those of many other types of cyberattacks; All that stands between a criminal and the money of victims in today's computerised commercial and financial environment is access credentials, credit card numbers, or personal data that can subsequently be utilised to commit identity theft (Fortinet, Inc., 2023). During the vishing attack, scammers usually use phone calls to get the targets to provide personal information. The Independent Online (2021) mentions that South Africans are urged to look out for vishing as one of the cybercrimes. Furthermore, the Independent online (2021) argues that these fraudsters impersonate bank representatives calling their targets and employ fear tactics to persuade them that their money is in jeopardy if they do not reveal their account or card details. Sometimes they even persuade some people to make payments themselves, assuring them that by doing so, they will be able to stop the alleged scam, while actually, the person is making payments to the fraudsters.

2.3.10 Distributed Denial-of-Service (DDoS) attack

Bhatia *et al*. (2019) describes distributed denial-of-service as a situation, often resulting from a deliberate and malicious attempt by an adversary to intentionally disrupt the normal operations of a service provider (or a server) and render the resources unavailable to its intended clients. Qadir and Quadri (2016) argues that the fundamental goal of Denial of Service (DoS) attacks is to make an information resource unavailable or to put it another way, to reduce information availability. For example, the banking industry was struck by a wave of ransomware-driven distributed denial of service attacks that targeted multiple banks' publicfacing services. Similarly, another example; PwC (2023), "A bank experiencing systems failure meant 600,000 customer payments and direct debits went missing. The failure was caused by the bank's IT infrastructure struggling to deal with traffic volumes.".

Additionally, Moyo (2019) states that the attacks began with delivering a ransom note via email to both unattended and staff email addresses, both of which were publicly accessible. Further, from the Johannesburg local government and finance sector hack one group sent a ransom note to several banks, threatening to conduct a distributed denial of service (DDoS) attack unless paid two Bitcoins valued at R219000 (Smillie, 2019).

2.3.11 Identity theft

Identity theft is described by Hussain and Cheng (2022) as the crime of obtaining the personal or financial information of another person to use their identity to commit fraud, such as making

unauthorised transactions or purchases and its victims are typically left with damage to their credit, finances, and reputation. Identity theft continues to be an issue for the country. Chigada (2020) argues that thieves are skilled at deciphering psychology, and they frequently employ social engineering techniques to take advantage of human weakness in gather private information like a personal identification number (PIN) or password.

2.3.12 Ransomware

The Threatpost (2021) argues that one of the most destructive fallacies regarding ransomware attacks is, "If your organisation does frequent system backups, you do not have to worry". After an attack, all that companies need to do is to restore information from the backup. Also, Threatpost (2021) states that while system backups are critical, power failures, natural disasters, and even personnel errors may wipe out data just as swiftly as a cyberattack, they are not an instant fix. Ascend IT Solutions, Inc. (2021) further adds that the impact of ransomware includes the following:

i. Temporary, and possibly permanent, loss of company's data, ii. Possibly a complete shutdown of the company's operations, iii. Financial loss as a result of revenue-generating operations being shut down, iv. Financial loss associated with remediation efforts,

v. Damage to company's reputation.

Ransomware is a type of malware that spreads like a worm and prevents or restricts users from using their system by locking the screen or encrypting and locking their files unless a ransom is paid (Shah and Farik, 2017). A ransomware attack is one of the biggest challenges in cybersecurity nationally. When companies pay ransomware, it is still possible for them to not get back their data. In 2021, 68.5% of businesses were victimised by ransomware, which was an increase from the previous three years and the highest figure reported so far (Statista, 2021). Companies need to develop strategies to prevent criminals from successfully attacking them.

The governments, educational institutions, telecommunications, industrial, finance, and business industries were hit by a powerful global ransomware attack through a Microsoft Windows operating system vulnerability (Venktess, 2017). Research shows that cybercriminals use the WannaCry virus, which tries to access a particular Uniform Resource

Locator (URL) after it has been installed; if it cannot access it for any purpose, it scans for and encrypts files in various formats, keeping them inaccessible to the user. In exchange for a key that would decrypt their data, attackers demanded that the targets pay roughly a ransom of about R4000. Research shows that in South Africa, at least 1000 computers were found to be vulnerable to the virus with no confirmation about how many were infected. Additionally, DebtIN consultants, a South African-based debt collector, was hit by an excellent ransom attack in April 2021. According to Debt-IN Consultants, more than 1.4 million South Africans' consumer and personal information was fraudulently accessed from Debt-IN servers in April (Moyo, 2021).

2.3.13 Software piracy

Khadka (2015) defines software piracy as a crime commonly defined as illegal copying, downloading, sharing, selling, or installing of copyrighted software. The Learningcurve (2017) states that during 2016 the companies in South Africa incurred more than R3.64 million in fines for using unlicensed software. The research revealed that 33% of software installed on computers in South Africa is not correctly licensed, representing a total value of $274 million. For example, Prior (2020) states that due to the COVID-19, there was an increase in online banking and e-commerce transactions, and cyber criminals took that as an opportunity to further their nefarious activities by convincing consumers that they are dealing with legitimate businesses or banks.

2.3.14 Salami slicing attack

Signh (2023) defines a "salami slicing attack" or "salami fraud" as an attack that occurs when an attacker uses an online database to obtain customer information, such as bank/credit card details. Over time, the attacker deducts insignificant amounts from each account. The staff reporter of the Moyo (2016) reported that the fraudsters made 14 000 transactions with fake credit cards cloned from the details of 1 600 Standard Bank customers in South Africa, withdrawing a total of R300 million in Japanese yen from 1 400 automated teller machines (ATMs) in just three hours. The whole incident was a loss to the bank but not the customers.

2.3.15 Trojans

Studies show that Russia, South Africa, and the United States had the most targeted users by android banking malware in 2018; the number of users attacked with banking Trojans was 889,452 – an increase of 15.9% in comparison with 767,072 the previous year (Intelligent CIO, 2019). By creating trojans, criminals aim to destroy, disrupt, steal, or otherwise harm data or

networks. BusinessTech (2021) warns about the three most prevalent banking malware behaviours that Kaspersky has seen in South Africa, namely;

i. Trojans

The Economic Times (2023) defines a trojan as a type of computer software disguised as ordinary software, such as utilities, games, and even antivirus programs. Once installed, it causes issues such as terminating background system activities, destroying data from hard drives, and corrupting file allocation systems.

ii. Trojan-Proxy

F-secure (2023) describes a trojan-proxy as a type of trojan that, once installed, allows an attacker to use the infected computer as a proxy to connect to the Internet. The proxy Trojan hijacks the user's browser when they access it, sending them to malicious websites or compelling them to download harmful files.

iii. Trojan-Downloaders

A trojan-downloader is a type of trojan that installs itself to the system and waits until an Internet connection becomes available to connect to a remote server or website to download additional programs (usually malware) onto the infected computer (F-secure, 2023).

2.3.16 Card fraud

Criminals who commit counterfeit debit and credit card fraud avoid EMV (personal identification number [PIN] or chip technology) by transitioning from card jamming and swapping at automated teller machines (ATMs) to steal cards to shoulder surfing to obtain PINs (Chigada, 2020). Moreover, Card Not Present (CNP) fraud accounted for 62% of total fraud losses on South African-issued credit cards in 2019, accompanied by False Applications (27.1%) and Counterfeit (5.7%) fraud (BusinessTech, 2020). Also, the gross losses due to fraud committed on South African-issued debit cards amounted to R520.5 million in 2020 - an increase of 26.5% compared to 2019 (Smith, 2021). Due to the COVID19 lockdown, most people opted to use online platforms for purchases, and criminals used that to their advantage. Smith (2019) further states that the widespread adoption of remote working has resulted in unprecedented technical vulnerabilities in network security and the adoption of online collaboration platforms.

2.3.17 Web jacking

Krunal (2023) states that web jacking vector is used in social media where the attackers create a fake website and when the website opens it will redirect it to another website and harm the users system. BusinessTech (2019) argues that international law enforcement investigated a complex cryptojacking scheme that included South African internet protocol (IP) addresses. Cryptojacking is defined as a malicious cryptomining that happens when cybercriminals hack into both business and personal computers, laptops, and mobile devices to install software and the software uses the computer's power and resources to mine for cryptocurrencies or steal cryptocurrency wallets owned by unsuspecting victims (Sobers, 2021). With the 60% of South African companies who experienced a public cloud security incident, the State of Cloud Security report in 2020 revealed that 26% of those attacks were cryptojacking. In addition, Grobler (2020) states that in Cape Town, a former barman at a well-known restaurant was arrested for cloning a customer's bank cards.

2.3.18 Smishing

Kaspersky Lab (2021) defines smishing as a social engineering attack that relies on exploiting human trust rather than technical exploits through the combination of Short Message Service (SMS) and phishing. Cybercriminals send fraudulent emails that trick the recipient into clicking on a malicious link. The Southern African Fraud Prevention Service (SAFPS) has raised concerns about the rise in impersonation crimes as fraudsters use phishing, smishing, and vishing to prey on their victims (ITWeb Limited, 2022).

2.3.19 ATM malware

ATM malware and jackpotting are attacks in which hackers reprogramme ATMs to disburse massive amounts of cash; the attack necessitates cyber criminals prying apart a component of the machine and connecting a computing device to the USB port to upload the jackpotting malware (Lindsey, 2019). Research shows that ATMs are vulnerable to hacks because they utilise the Windows XP operating system, which Microsoft no longer supports. Alfreds (2016) states that the SABRIC has encouraged bank clients to be wary of suspicious people near ATMs and to refuse aid from strangers and recommended that bank customers be cautious of altered display layouts on ATM screens since this could indicate tampering, and to avoid forcing cards into machine slots.

2.4 Effects of cybercrime

The report, which was produced in collaboration with the Center for Strategic and International Studies (CSIS), estimates that cybercrime costs the global economy more than $1 trillion, or just over 1% of global GDP, an increase of more than 50% from a 2018 study that estimated global losses at around $600 billion (Smith and Lostri, 2020). Cybercrime affects organisations significantly. The following figure shows the six impacts of cybercrime on businesses.

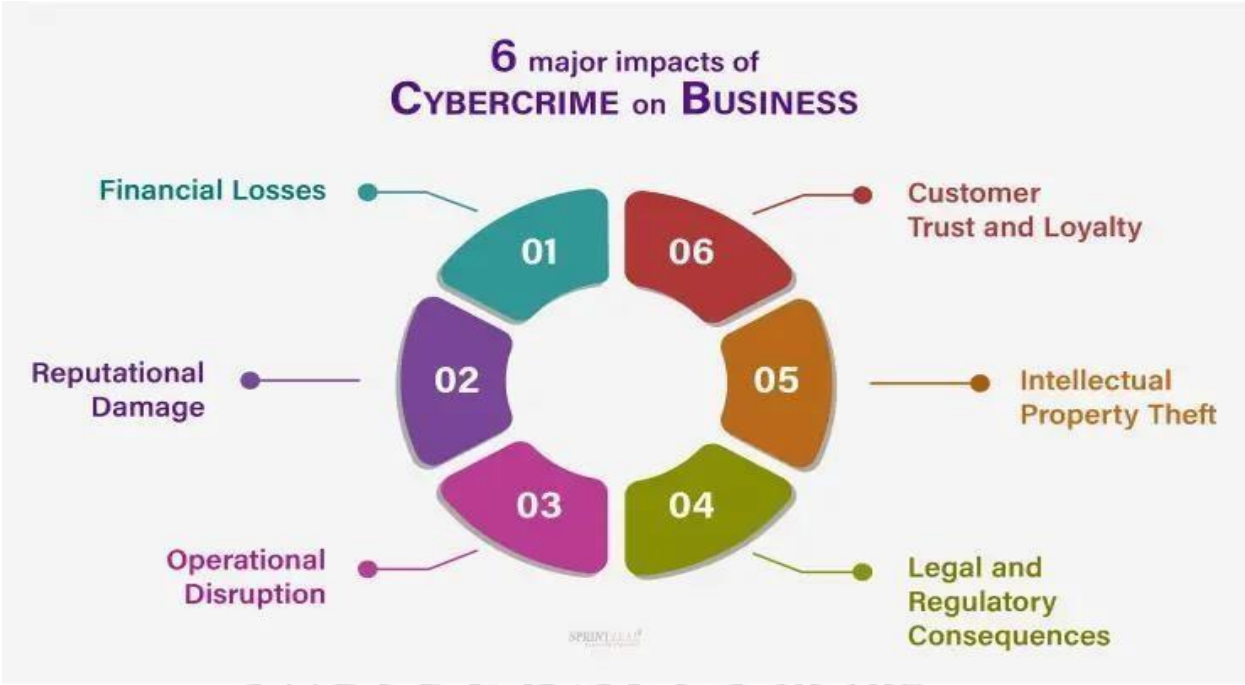


Figure 1: 6 major impacts of Cybercrime on Business (Source: Sprintzeal Americas Inc., 2023)

i. Financial Losses

All cyberattacks can have a disruptive effect on business processes but notably of denialofservice attacks, malware, and spam. These disruptions cause firms to lose production and miss out on sales, and they frequently have repercussions for other companies in the same supply chain (Gañán, Ciere, and Eeten, 2017). Comparably, Unni (2022) states that a hacker can simply drain the bank accounts if they can access them and hackers during ransomware attacks can demand a financial payout in order to end a Denial-of-Service scenario. Additionally, firms may have to pay for a range of expenses, such as cybersecurity technology and expertise, breach notification, insurance premiums, public relations support, and the hiring of lawyers and other specialists to stay in compliance with cybersecurity requirements.

ii. Reputational Damage

The cybersecurity breaches known by the public can result to reputational damage. An example provided by Gañán, Ciere, and Eeten (2017) is that customers may stop using the service from an organisation that experienced the breach. The cost of such reputation damage mostly consists of the lost market share and the expenses on public relations measures. Further, Carnal (2023) argues that a company's reputation may suffer to the point where potential business partners or investors become hesitant to engage in new ventures; this can lead to missed opportunities for growth and collaboration, ultimately hampering the company's long-term success.

iii. Operational Disruption

Cyberattacks often have indirect costs, such as the likelihood of a severe disruption in operations, which can result in revenue loss. Kaput (2023) states that while conventional cybercrimes, such as viruses and Trojan worms, can cause a company's website to malfunction or its computers to malfunction, even more, insidious cybercrimes, such as denial of service attacks, can do even more damage by bringing a company's operations to a standstill.

iv. Legal and Regulatory Consequences

Sprintzeal Americas Inc. (2023) argues that cybercrime carries legal and regulatory implications for businesses, which can result in severe penalties and legal actions. For example, Dosal (2023) states that in some cases, customers may file lawsuits against the company for failing to meet their security obligations.

v. Intellectual Property Theft

Most companies store intellectual property on the cloud, which is vulnerable to attacks. Theft of company resources such as trade secrets, trademarks, and copyrighted information lowers the organisation's competitive advantage. As stated below by Sprintzeal Americas Inc. (2023), are the impacts of the theft of intellectual property.

- Loss of Competitive Advantage: Competitors may get an unfair advantage as a result of stolen intellectual property, which could lead to a loss of market share, decreased profitability, and decreased innovation.
- Reputational harm: Theft of intellectual property can damage a company's reputation because stakeholders may doubt its capacity to protect priceless assets.

vi. Customer loyalty and trust

Dosal (2023) states that cybersecurity breaches can lead to a loss of trust in the company and negative publicity that could damage its brand and reputation. It can be difficult and expensive to repair, so businesses should take all possible precautions to protect themselves and their customers from cyber threats. Moreover, a successful cyberattack reveals a business's negligence in safeguarding confidential data of its clients, resulting in a substantial decline in trust (Carnal, 2023). This means that the customers and suppliers may be hesitant to entrust their sensitive data to a company whose IT system has been breached.

Further, banks and their clients face significant reputational and financial threats due to vulnerabilities in financial web applications (Financial Application, 2018). With financial institutions being exposed to security vulnerabilities, hackers can access clients' personal information and, in some cases, confidential banking details, which could lead to significant losses for the firms. In addition, Uddin *et al.* (2020) states that the effects of a cyberbreach and malicious activities may reach far away from the measurable direct financial losses due to the direct and indirect costs for the loss of customers' confidence, opportunity costs for service breakdown, costs for incidence detection and cleaning up in the aftermath of cybercrime, costs associated with the loss of confidential business information and intellectual property, and loss of reputational damage of the hacked institution (). Hence, the banks and other financial institutions need to ensure that proper encryption is used for all data and required training for the best security is provided to the employees. In the financial industry, investigations by the responsible regulatory bodies are conducted following a data breach, which could also lead to license termination for the affected organisations are always (Matters, 2016).

2.5 The South African cybersecurity landscape

Chipeta (2022) argues that the increasingly sophisticated tools and attack methods, greater reliance on information technology products and services (such as SaaS offerings), networks that encourage and enable the distribution of cybercrime profits (such as the dark web), greater availability of skills, personnel, and finances to drive cyberattacks , faster software releases with added functionality, new hardware development (such as Internet of Things (IoT) devices) and external factors (such as a global pandemic or financial crisis) are the main factors contributing to the dynamic threat landscape. Organisations must stay updated about the cyber threat landscape to be able to know the potential risks to them. The cybersecurity landscape also helps firms to prepare measures for protecting against attacks. The top threats in 2022 include the rise in social engineering such as the use of deepfake capabilities continues to grow, business email compromise, and third-party risks (Doyle, 2022). Remote working also

broadened organisations' attack surfaces dramatically and bringing-Your-OwnDevice (BYOD) policies introduced new attack vectors (Chipeta 2022).

Organisations such as financial institutions have adopted the use of digital transformation to create new and or enhance current business processes, culture, and consumer experience. As organizations digitise their operations, data becomes their lifeblood, from sensitive customer information to proprietary business strategies, safeguarding data is paramount (Sabu, 2023). Businesses have seen a significant increase in security events during the last two years, more especially during the period of COVID-19 where employees had to work from home. Mokoka (2020) states that although South Africa is more cybersecure than it was in the previous year (2019), it remains vulnerable; countries were ranked from one to 76, with one being the least cybersecure and 76 being the most secure, South Africa, which was ranked in position 29 in the world in 2019 and ranked in position 31 in 2020. The analysis focused on cyber aspects such as malware infection rates, the amount of financial malware attacks, cyberattack preparedness, and cybersecurity legislation.

Winder (2021) argues that while cybersecurity was never omitted from the digital transformation process, accelerated implementation timelines meant blind spots were created; as firms increasingly use hybrid work models, such flaws must be addressed by the C-suite, ensuring that cybersecurity is baked in going forward. In addition, the BusinessTech (2021) states that 85% of South African companies had experienced a business disruption, financial loss or other setback in 2020 due to a lack of cyber preparedness. Additionally, the Mimecast State of Email Security 2022 report, which analyses responses from 1400 IT and cybersecurity professionals across 12 different countries, reveals that South African organisations devote on average only 12% of their IT budgets to cyber resilience, which is less than the global average of 14% (ITWeb Security Summit, 2023). The study conducted FTI Consulting Inc. (2020) among the G20 countries shows that companies in the region are more vulnerable to cyber assaults and ransomware than global averages (33% vs. 27% for overall attacks). Furthermore, the research conducted by FTI Consulting Inc. (2020) shows that majority of leaders in the region are aware of the risks (84% say they have cybersecurity vulnerabilities), just about half of the leaders surveyed made investments in that area of their firm in the recent year. Like in other countries, the lack of readiness for cybersecurity in South Africa remains a major issue that needs to be addressed.

Pygma Consulting (2023) South Africa, like the rest of Africa, is falling behind in terms of cybersecurity, and its government is grappling with issues such as a lack of ICT skills and

coordination between inter-governmental departments. However, research shows that despite efforts to update and reinforce cybersecurity legislation and procedures in South Africa, significant loopholes persist. Also, Reese (2021) states that cybersecurity gap is a multifaced problem as many small to midsize organisations don't properly prioritise cybersecurity and companies that have open cyber roles do not know how to fill them. Without a question, South Africa as well as other countries with poor cybersecurity implementation, with the assistance of its government, have much more work to do to ensure that these issues are reduced.

2.5.1 The lack of preparedness for cybersecurity

Preparedness means proper planning, resource allocation, and training, including simulated disaster response exercises (Laaser, and Beluli, 2016) Also, the Office for the Coordination of Humanitarian Affairs (OCHA) (2016) defines preparedness as the ability of governments, professional response organisations, communities, and individuals to foresee and successfully respond to the effects of likely, imminent, or current risks, events, or situations. Organisational readiness entails putting in place processes that allow them to be aware of the risks and promptly deploy personnel and resources when a crisis occurs. Bonime-blanc and Saban (2021) states that the cyber-crisis preparedness is an important part of broader cyberresilience, no matter how big or small your organisation.

In Cybersecurity, Graham (2021) states that readiness can identify, prevent, and respond to cyber threats. Similarly, Cybersecurity preparedness refers to any measures that contribute to an organisation's readiness and ability to respond to or recover from an incident affecting its IT or OT systems, such as designing and practicing plans or training and equipping employees (Cadmus Group Llc, 2019). Firms need to be prepared at all times to ensure that they will manage to continue with operations and not endure too much loss or even none after any incident. The organisational lack of readiness to combat the cyberattacks leads to them experiencing financial and data losses; this can harm the entire reputation and negatively impact the company's performance. Additionally, the lack of preparedness means that companies have no strategies in place that enable them to detect a cyber-attack before or during its occurrence and recover from it. It leaves businesses vulnerable to attacks.

Voses (2019) advises the companies to do the following to prepare and protect against cyberattacks. Firstly, physically, and electronically securing your servers and conducting ongoing risk assessments. Secondly, requiring background checks on contractors given access to computer system and thirdly, investing in Endpoint Detection and Response, logs, Security Information and Event Management, and Network Detection and Response; with

such, organisations can invest on Intrusion Detection Systems (IDS). Sarker *et al.* (2020) states that IDS, a) monitors and assesses normal network or computer system activity to find security risks or threats like denial-of-service (DoS), b) performs the process of recognizing malicious cyber-attack behaviour, and c) helps to discover, determine and identify unauthorised system behaviour such as unauthorised access, or modification and destruction. Firms are further advised to require their vendors to maintain robust cybersecurity and certify their efforts at compliance. Lastly, have an incident response plan now because the time to prepare has passed when a problem arises.

Moreover, Bonime-Blanc and Saban (2021) discusses the five T's of organisational cybercrisis readiness as talent and planning, technology and infosec governance, training and communication, technology tools, and triangulation and continuous improvement.

i. Talent and planning

The most important aspect of cybersecurity preparedness is having adequate people preparing by gathering around a virtual or actual table, practicing for cyber crises, and dealing with them when they occur. Cohanim (2023) adds that with centralised, effective management and planning, organisations can gain insights into employee skills, competencies, and knowledge, align them with specific roles and responsibilities, identify skill gaps, offer targeted training and development programs, and ensure greater cyber readiness.

ii. Technology and infosec governance

Organisations needs to have a method of how a company evaluates, defends, and interferes with all things digital within its reach. Federal authorities such as Certified Information Systems Auditor (CISA), for instance, concentrate on cybersecurity governance frameworks in order to assist organisations in managing security risks (Hammer, 2024). Additionally, Hammer (2024) mentions tools like Centraleyes, which can help organisations streamline governance, move away from manual processes, and add value to managing security incidents.

iii. Training and communication

Organisation should have a computer security education strategy in place, with regular testing of the system and training of personnel and third parties on the things they are supposed to do in case of cyber-attack. For example, The RangeForce team (2024) states that hands-on skills development can help improve collaboration and communication by fostering a shared understanding of cyber threats and the best practices for defending against them. The

RangeForce team (2024) points out that improved communication can lead to better solutions for issues relating to cybersecurity or threats that arise during operations.

iv. Technology tools

As the people, governance, training and communications pieces of a cyber-crisis plan take shape, Bonime-Blanc and Saban (2021) states that it is important for the cybersecurity team of an organisation to plan and have a clear understanding of and a map of all the necessary and desirable technology tools in use across the firm, both in advance of a major cybercrisis and for purposes of maintaining post-crisis business continuity.

v. Triangulation and continuous improvement

Every entity's cyber-crisis readiness approach should include a set of critical system-wide practices and policies that help identify, mitigate, and resolve issues, ideally before they occur but frequently afterward as well. Graham (2023), for example, states that organisations can use tools like security ratings to continuously monitor the digital ecosystem. Graham (2023) explains that security ratings are derived from objective and verifiable information , which can help organisations assess risk and the likelihood of a data breach based on risk factors such as open ports, misconfigured software, malware infections, exposed credentials, and weak security controls.

2.5.2 How to assess the preparedness of the firm

Firms need to constantly assess their preparedness to deal with the cybersecurity issues and business continuity after an incident. Graham (2021) states the following as the ways in which organisations can evaluate their cybersecurity readiness;

2.5.2.1 Continuously assess company's cybersecurity readiness

New threats emerge all the time, malicious actors are constantly seeking security flaws, and the security team's work is never "done."; no organisation is truly safe or secure in the knowledge that it will not be attacked (Richmond, 2017). Hence firms need to assess their preparedness for cybersecurity challenges constantly. Graham (2021) mentions that regular audits and assessments are a tried and tested way to evaluate cybersecurity readiness; however, these are limited as they capture only a point-in-time view of company security posture. Moreover, Graham (2021) states that a better way to assess cyber risk is by continuously monitoring the digital ecosystem using a tool like security ratings.

2.5.2.2 Evaluate the cybersecurity readiness of your vendors

Organisations are dependent on vendors for some of the services. Companies must evaluate vendors' cybersecurity readiness as weak vendor security controls might lead to the company systems they have access to being vulnerable. For example, PwC (2023) mentions that third-party data breaches may force an organisation to respond to incidents that are outside of its control or originate from an indirect source; even though existing breach standards do not require the organisation to respond, the firm may nonetheless sustain serious reputational harm as a result of the occurrence. Tunggal (2023) states that vendor risk management focuses on mitigating the risk of being exposed to or financial losses as a result of a cyberattack, data breach, or another security incident. This risk is frequently minimised by conducting due diligence prior to bringing in new vendors and continuing to monitor them during their lifecycle.

2.5.2.3 Develop a realistic incident response plan

The incident response plan helps firms detect, respond to, and recover from network security incidents. Graham (2021) argues that organisations often concentrate their risk mitigation efforts on improving security controls while neglecting to anticipate how they will respond if an attack occurs, resulting in significant delays in discovery and recovery. Steps to creating an incident plan include choosing an incident response planning consultant, assessing the company's current risks, identifying the response team, preparing, and training the incident response team, and improving and evolving the organisation plan (Blankenship, 2021).

2.5.2.4 Approach cybersecurity readiness as everyone's responsibility

Most cyberattacks involve the human element, hence the increased urge for organisations to train and educate employees about cybersecurity issues. Borza (2021) states that modern attacks occur on several levels, and they are no longer solely technological; criminals are also leveraging company staff against the company, although the majority of them have no idea what they are doing. The V-Soft Consulting (1997-2021) further argues that combating cybersecurity challenges is a shared responsibility in a company; it should be strengthened at enterprise management and worker levels. Strengthening cybersecurity among employees ensures that they take accountability in protecting sensitive information.

Hartwig (2021) states that for companies to increase cybersecurity awareness among the employees, they need to make it a responsibility of one group of employees to organise cybersecurity education and training to promote awareness. Also, for employees to know when

they receive emails that look out of the ordinary and ensure to verify the sender, companies should educate employees on all types of phishing and cyber scams. Moreover, firms can try to keep sensitive data secure and restrict access to it. Lastly, the companies can provide essential tools such as reverse lookup, antivirus, firewalls, intrusion detection, and VPNs, and data encryption to the employees.

2.5.3 Cybersecurity challenges

The cybersecurity challenges are discussed below.

2.5.3.1 More complex cybercrimes

There is an increased reliance on software, hardware, and cloud infrastructure, as well as rapid use of machine learning and artificial intelligence capabilities. This means that organisations, including financial institutions, and people should be wary more of cyber criminals.

2.5.3.2 Software vulnerabilities

Software vulnerabilities are weaknesses in software that malicious actors can exploit to get access to a network's sensitive data. The firm's main concern should be keeping a device's software up to date as older software version may include patches for security flaws that have been addressed by the developers in a modified version. According to Ashley (2021) the following are the most common software vulnerabilities; insufficient logging and monitoring, injection flaws, sensitive data exposure, using components with known vulnerabilities, crosssite scripting (XSS) flaws, broken authentication, broken access control, xml external entities (XXE), security misconfiguration, and insecure deserialisation.

2.5.3.3 Legacy systems

The new updates required to mitigate software vulnerabilities may not be compatible with the device's hardware; this is what leads to outdated hardware, which is not capable of running the most recent software versions. Outdated hardware is more vulnerable to cyber threats. Ancell (2021) states that businesses that use outdated legacy technology increase their cybersecurity vulnerabilities and as a result, over 10,000 new malware threats are discovered each hour.

2.5.3.4 Fragmented and complex regulations

Taherdoost (2022) suggests that cybersecurity standards determine the requirements that an organisation should follow to achieve cybersecurity objectives and facilitate against cybercrimes and demonstrate whether an information system can meet security requirements

through a range of best practices and procedures. However, regulations can burden business owners with "*fragmented*" and "*conflicting*" priorities, as they must "*defend and protect against attacks while still attempting to comply with complex regulations*", (Intellesec, 2021). Additionally, Cin and Jurgens (2023) point out that the large increase in cyber incidents, related fines, investigations and engagements between policymakers and the private sector has elevated the perception of regulations as a critical influence on organisations' cyber resilience. Hence policy makers need to ensure that innovative policies are in order to provide more protection while reducing regulatory complexity. Furthermore, Terry (2022) in the literature stated that regulators require that financial institutions adhere to a wide range of cybersecurity compliance standards; regrettably, there are divergent expectations across regulators, which makes it more challenging for financial institutions to set clear goals.

2.5.3.5 Outsourcing

Businesses are becoming increasingly reliant on some technological providers; with this, an ecosystem is only as strong as its weakest link (Intellesec, 2021). SMBs must ensure they have an adequate amount of visibility and awareness of digital assets as this gives access points for attackers.

2.5.3.6 Difficulty tracking cyber criminals

Studies show that being a cybercriminal comes with a lot of benefits and little risks because, until recently, the likelihood of being caught and prosecuted as a cybercriminal in the United States was thought to be as low as 0.05%. In several other countries, the percentage is significantly smaller. TMB Managed IT Services (2022) suggests the following challenges as what makes it difficult to catch cybercriminals:

i. Jurisdiction

The main challenge is that the parties to a dispute are essentially located in separate parts of the world and have just a virtual connection that brings them all together into one domain. Also, most countries do not want their citizens to be at the mercy of other legal systems, and without extradition laws in place, foreign governments are often unwilling to cooperate. In the case of South Africa, Tredger (2023) mentions that the lack of requisite skills and an immature judicial system could hinder efforts to enforce South Arica's Cyber Crimes Act. Tredger (2023) explains that law enforcement needs more capacity building to adequately deal with cyber security incidents, victims and processes such as forensics and securing evidence chains.

ii. Proxies and other technology

Cybercriminals that are cautious will go to considerable measures to conceal their identity and location; they often do business on the dark web, which makes it difficult to track them. Technologies such as Tor software and encryption enable hackers to add multiple layers to mask their identity (Mackay, 2024). Furthermore, cybercriminals hide their true internet protocol (IP) address via virtual private networks (VPNs) and proxies, making it incredibly difficult to determine their true location. Mackay (2024) explains that secure software such as a proxy server helps hackers hide their identity and funnel their communications through lots of different countries in order to evade detection.

iii. Inadequate Laws

New regulations must be enacted, in order to stay up with the latest technologies as one cannot be accused of committing a crime if their actions have never been classified as one (TMB Managed IT Services, 2022). Cybercriminals take advantage of the fact that cybercrime regulations and law enforcement training are inadequate in developing countries (ITWeb Security Summit, 2023). Although South Africa's Cyber Crime Bill was signed into law in 2021, the ITWeb Security Summit (2023) points out that many cyber police officers continue to lack sufficient training.

iv. Lack of Reporting

According to one of the primary obligations of the GDPR, companies must report cyber breaches in a timely manner. The issue is that companies are frequently hesitant to disclose they have been hacked; it makes them appear unprofessional, and it may turn off potential customers (TMB Managed IT Services, 2022).

2.5.3.7 Lack of cybersecurity expertise

Most countries are lacking cybersecurity professionals which makes it difficult for organisations to prepare and be updated about latest cybersecurity issues. de Jager, Futcher, and Thomson (2023) mentions that there are several challenges, such as lack of time, lack of funding and lack of resources, that South Africa must overcome in order to address the cybersecurity skills gap. Organisations should prepare for cyberattacks by anticipating they will be struck, backing up IT resources and data, ensuring business continuity in the case of computer system failures, and drilling and training the organisation in realistic cyber response strategies. Palmer (2021) warns that the lack of business investment combined with the challenge of additional workloads results in skills shortage that's leading to unfilled jobs and high burnout among information security staff. Over and above that, Palmer (2021) discovered that 57% of cybersecurity professionals mentioned that a shortage of cybersecurity skills has impacted the

organisation they work for, while just over 10% report a significant impact. As concern in companies that they are becoming the most targets for cybercriminals increase, therefore bridging the gap between supply and demand for cybersecurity professions is critical. O'dea (2021) argues that IT security specialists, information security analysts, network security engineers, security engineers, and application security engineers are among the jobs with the highest skill shortages. Research by Buckbee (2021) reveals that the factors that lead to the key shortage of skills in the field include the rising frequency of cyberattacks, a lack of skilled defenders against cybercrime, lack of interest among younger generations in a cybersecurity profession, and a significant employee turnover due to burnout. Additionally, lack of skills in diversity in the cybersecurity space contributes to the shortage of skills in the field. According to the International Information System Security Certification Consortium (ISC) 2 Global Information Security Workforce Study (2021) a reliable estimate of women in the cybersecurity workforce globally remains at 25% while men take up 75% of the industry and that makes this industry male-dominated. Amos (2022) mentions that a diverse team could be highly useful, even though it is important to consider a person's experience and education.

One of reasons why cybersecurity has not been able to achieve some level of gender equality is that there is still a preconception that technical professions are the best options for boys, not girls, among young girls and even their families (CyberWarrior 2023). Over the years, women have joined the industry, however, Chamlou (2022) suggests that the recent increase in the number of women and people of colour of all genders working in cybersecurity still does not improve diversity in firms as these groups are still underrepresented in the industry.

Dallaway (2016) states that it was suggested that women bring a different mind-set and set of skills to the workplace, including attention to detail, analytical ability, and problem solving.

In research, Oltsik (2021) discusses the 7 key data points on the cybersecurity skills shortage as:

Most organisations are impacted: 62% of those impacted said the skills scarcity has increased the workload on existing staff; 38% said new security roles remain unfilled for weeks or months; and 38% said the skills deficit has resulted in employee burnout and attrition.

The skills shortage is not improving: The cybersecurity skills gap (and its impact) has gotten worse for 44% of poll respondents in the last few years, while 51% believe it is about the same today as it was a few years ago. Unfortunately, only 5% say the situation has improved.

Recruiting and hiring cybersecurity staff remains challenging: Recruiting cybersecurity specialists is either extremely tough or fairly challenging for security professionals. Studies reveal that businesses across the world are finding it difficult to find and keep skilled cybersecurity expertise as the skills gap widens (Skelton, 2022).

There is an acute shortage of cloud security and other skills: The most acute skills need is said to be in cloud computing security, followed by application security and/or security analysis and investigations.

Organisations are not doing enough to bridge the cybersecurity skills gap: In the study Oltsik (2021) conducted, the findings show that 27% of survey respondents believe their company could do more to solve the skills gap, while almost one-third (32%) of the respondents believe their company could do a lot more.

The cybersecurity skills shortage exposes organisational issues: The research revealed that some company human resources staff does not understand cybersecurity skills, so suitable individuals are likely to be overlooked, while some say cybersecurity job advertisements are unrealistic, requiring too much experience, too many certificates, and so on.

Cybersecurity professionals have some helpful recommendations: When asked what more their companies might do to solve the skills gap, cybersecurity experts suggested increasing their commitment to cybersecurity training, increasing remuneration, providing additional perks, and launching or improving a cybersecurity internship program.

2.5.3.8 Unskilled and inexperienced technology users

The unskilled and inexperienced technology users are the individuals who are do not have much knowledge in using technology. Most companies have adopted online services, which give their customers access to some of their systems. Hence, hackers tend to target the company clients as most users do not have security controls protecting against cyber threats, leaving customer devices vulnerable to attacks. Chase (2021) states that customers that use the internet and mobile-centric products and services pose a specific risk to your company, necessitating the implementation of additional controls to manage client risk; most organisations cannot make clients follow the rules and processes that are not part of the products they are using. Similarly, while threat actors continue to attempt to exploit digital platforms such as banking sites or other locations that contain financial data, the mitigation

techniques employed by these companies are typically robust—it is easier to target individuals due to their lack of technological expertise (Mcanyana *et al*., 2020).

Organisations are more focused on adopting cybersecurity within their operations without raising awareness to other parties, such as their clients, on the security issues and how they can ensure that they do not fall victims. Some of the most severe cybersecurity threats originate from a lack of consumer awareness, especially when it comes to securing personal data. A lack of consumer knowledge, particularly when it comes to securing personal data, is at the root of some of the most significant cybersecurity concerns (Clements, 2020). The poor public knowledge on cybersecurity issues remains a big issue in South Africa.

Crellin (2015) lists the seven ways for companies to rise cybersecurity awareness among their customer as follows:

i. Use stats to communicate the importance of cybersecurity

Using the statistics to raise awareness about cyber threats might show the consumers how significant it is to protect against cyberattacks. Dolley (2021) states that South Africa's vulnerability to hackers and ransomware attacks, which pose a threat to individuals, the economy, and infrastructure, has been demonstrated through the recent cyberattacks. Research shows that South Africa is rapidly being targeted by online criminals, which now have the world's third-highest number of cybercrime victims.

ii. Teach end users how to protect themselves from cybercrime

Organisations can start showing consumers how to disable attachment auto-downloads and save and scan attachments before opening them will help prevent an incident.

iii. Share examples of what an attack might look like

Providing examples of typical attacks makes online safety training more effective. Also, companies should show customers what their system would look like if it were infected with malware to spot the warning signs and know to notify someone right away.

iv. Keep customers informed about current threats

Companies can accomplish this by sending out an email blast or organizing a webinar and adding a cybersecurity section in their customer newsletter.

v. Schedule regular refreshers and tests with customers' employees

Companies should use the time to discuss password management best practices and avoid phishing and keylogger frauds. Also, to encourage individuals to participate, companies can offer rewards to employees with the highest scores.

vi. Encourage your customers' employees to share potential errors right away Unintentionally clicking on a malicious link is an excellent example of situations whereby an employee or consumer can make an error, and by reporting it right away, the employee can reduce the time between the possible breach and its resolution.

vii. Periodically assess your customers' security posture

The CompTIA IT Security Assessment Wizard is a valuable tool that companies can use to assess company clients' IT security strengths and weaknesses to help them make changes to safeguard their organisations better.

2.5.4 Developing and enforcing strategies and processes

The Microsoft partner (2022) argues that cybersecurity is challenging as risk management is a complex topic requiring significant organisational involvement. The three pillars of cybersecurity help companies to have an effective strategy to protect against malicious actors. The three pillars are people, processes, and technology. Best Practice Certification Pty Ltd (2021) states that assuring that all employees understand their cybersecurity roles and are aware of workplace policies to mitigate and respond to cyberattacks is a critical step in preventing and minimizing cyber risks. Also, to reduce and limit the risk of cybersecurity threats, processes should describe the organisation's actions, roles, and documentation, and the company should follow a specific protocol (Roohparvar, 2019). Furthermore, the Charter college (2022) describes technology with cybersecurity as the mechanisms IT people build processes around to prevent compromises to an IT infrastructure; these include behaviour analytics, breach detection, and authentication response system.

2.5.4.1 Strategies for ensuring cybersecurity in an organisation

i. Creating a secure cyber ecosystem

IGI Global (1988-2023) defines an information security ecosystem as the network of entities that influence information security products and services. The information security ecosystem includes hardware and software vendors, consultants, digital forensics experts, standardisation agencies, accreditation and education facilities, academic conferences, and journals, books, magazines, hackers, and their miscellaneous articles (IGI Global, 19882023).

It helps maintain effective interaction between the parties involved in the cybersecurity infrastructure.

ii. Creating an Assurance Framework

Zhang (2020) argues that the ICS information security assurance framework is created to integrate both technology and management, taking full consideration of the enterprise's business requirements and ICS operating characteristics in response to associated compliance requirements put up by the industry and the country. The framework helps organisations create an outline that adheres to the international security standards requirements using traditional products, procedures, people, and technology. Moreover, the

iii. Encouraging Open Standards

Standards play an important role in establishing how organisations tackle information security concerns in different countries.

iv. Strengthening the Regulatory Framework

The strategy aims to develop a secure cyberspace ecosystem and strengthen the regulatory framework.

v. Creating Mechanisms for IT Security

Studies show that link-oriented security measures, end-to-end security measures, association-oriented measures, and data encryption are some of the core processes to ensure IT security. The strategy helps develop national-level systems, procedures, structures, and methods for generating realistic scenarios of current and potential cybersecurity risks and enabling prompt information sharing for individual institutions' proactive, preventative, and protective actions.

vi. Securing E-Governance Services

This strategy helps countries ensure that e-Government efforts incorporate global security best practices, business continuity management, and a cyber crisis management plan to reduce the risk of interruption and improve cyber resilience.

vii. Protecting Critical Information Infrastructure

According to the Global Forum on Cyber Expertise [GFCE] (2023), it is more important to protect the Critical Information Infrastructures such as telecommunications and data networks, financial systems and process control systems, because these don not just cross borders, but are connected to every other part of the world, through the internet and other networks. GFCE (2023) further explains that this means these critical information infrastructures are all

dependent on each other's security, as the weakest link can cause vulnerabilities for many others. It is therefore of ever-increasing importance to us all. This strategy secures data, database, network, communications infrastructure against cyber threats.

2.6 Cybersecurity

The Cybersecurity and Infrastructure Security Agency (CISA) (2019) defines cybersecurity as the process of protecting networks, devices, and data from unauthorised access or illegal use and maintaining the confidentiality, integrity, and accessibility of information. The International Telecommunication Union [ITU] (2018;2019;2020) argues that cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the cyber environment and organisation and user's assets. When planning to implement cybersecurity, it is important that the business understands and agree to the adoption of it; the strategy must align with the business goals. Despite the fact that boardroom discussion of cybersecurity is increasing, many CISOs still struggle to gain executive support and understanding since various board members frequently have varying opinions on what cybersecurity is and how it relates to privacy, data protection, and regulatory risk and others focus on risk postures, but few have an in-depth grasp of cybersecurity (Daswani and Elbayadi (2021).

As much as technological advancements bring considerable convenience to society, it still brings enormous harm. Seemma, Nandhini, and Sowmiya (2018) state that firms need cybersecurity to prevent cyber terrorism, cyber warfare, and cyber espionage threats. Cybercriminals target organisations because of their use of digital transformation. The newly integrated systems like business systems, Information Technology, and operational technology, which facilitate datadriven decision-making, generate more security concerns as these systems can also increase the speed and harm of attacks across business networks (Nguyen-Duy, 2018). This shows the great need for information systems security among companies that have adopted the technology. Truth (2019) argues that speed is one of the fundamental goals of digital transformation. The desire to transform can quickly lead businesses to compromise on security checks and ignore the underlying risks. Due to the ignorance of the underlying risks, corporates are left vulnerable to cyber threats and attacks. Truth (2019) states that data security, application security, visibility and analytics, digital infrastructure security, cloud security, and identity and access governance are technical pillars that impact digital transformation.

The enormous dissemination of connected devices in the IoT has produced tremendous demand for robust protection in response to rising demand from millions or possibly billions of connected devices and services globally (Abomhara, Køien and Alghamdi, 2015). It is significant to secure the IoT devices; cybercriminals attack firms through devices used by employees and consumers. Ervural and Ervural (2018) state that the future of cybersecurity relies significantly on considering threat landscapes and emerging developments in technology related to big data, cognitive computing, and IoT. Furthermore, it is important that organisations ensure security at all layers. Layered defense is the concept of securing a computer network using a number of defensive tools such that, in the event that one fails, additional tools are already in place to block an attack (Chellappan *et al*., 2015).

2.6.1 Cybersecurity concepts

i. The Confidentiality, Integrity and Availability (CIA) triad

The CIA triad is used as a guide when protecting data, software, and networks from security breaches. Nweke (2017) argues that confidentiality is concerned with viewing of data or information because if the wrong people see data or information they are not authorised, many problems could arise. Additionally, integrity refers to the completeness and accuracy of data, as well as the organisation's ability to protect it from corruption and availability as the ability to access information when needed (Irwin, 2023). Further, Fruhlinger (2020) provides the below example of how a CIA works in bank ATM:

- It provides confidentiality by requiring two-factor authentication (both a physical card and a PIN code) before allowing access to data.
- The ATM and bank software enforce data integrity by ensuring that any transfers or withdrawals made via the machine are reflected in the accounting for the user's bank account.
- The machine provides availability because it is in a public place and is accessible even when the bank branch is closed.

ii. Identity and Access Management

Dhamdhere, Karande, Phatak (2017) describe IAM system as a framework for business processes that facilitates the management of electronic identities and includes the technology needed to support identity management. In a workplace environment, De Groot (2019) states that when a user put their login details, a database is used to confirm the user's identity and determine whether the credentials entered match those in the database. IAM technology can

be used to initiate, capture, record and manage user identities and their related access permissions in an automated fashion; this ensures that access privileges are granted according to one interpretation of policy and all individuals and services are properly authenticated, authorised, and audited (Dhamdhere, Karande and Phatak, 2017).

iii. Security Information and Event Management (SIEM)

Vielberth (2021) mentions that an SIEM is responsible for collecting security-relevant data in a centralized manner to detect threats or incidents. As the SIEM receive events from many sensors (such as intrusion detection systems, antivirus software, firewalls, etc.), correlate these events, and present synthetic views of the alerts for threat handling and security reporting, they serve as the foundation of modern security operations centers (GonzálezGranadillo, González-Zarzosa and Diaz, 2021). In a workplace environment, it is used to monitor and capture an unusual behaviour on the network by the Security Operations Center.

iv. Advanced Persistent Threat (APT)

APT attacks are conducted with the goal of data theft rather than disrupting the organisation or network and once within the network, an attacker infects the target computer with APT malware (Khaleefa and Abdulah, 2022). APT attacks are designed to hide and lurk in a victim's network for weeks, months, and potentially even years (Ledesma, 2022). The figure below illustrates the lifecycle of APTs.

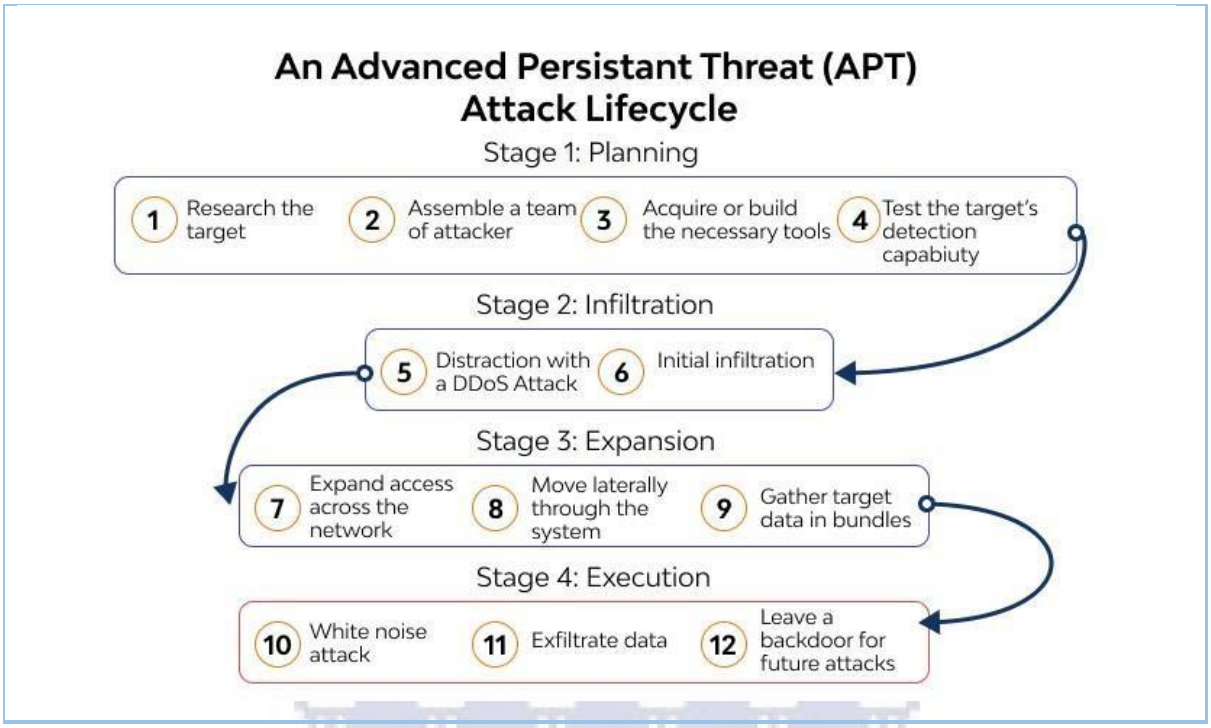


Figure 2: An Advanced Persistent Threat (APT) Attack Lifecycle (Source: Wallarm Inc, 2023)

v. User and Entity Behaviour Analysis (UEBA)

The Fortinet, Inc. (2023) describes UEBA as a cybersecurity solution that uses algorithms and machine learning to detect anomalies in the behaviour of not only the users in a corporate network but also the routers, servers, and endpoints in that network. For example, if a particular user on the network regularly downloads files of 20 MB every day but starts downloading 4 GB of files, the UEBA system would consider this an anomaly and either alert an IT administrator, or if automations are in place, automatically disconnect that user from the network (Fortinet, Inc., 2023).

2.6.2 Security risk assessment

IT Governance (2023) describes a cybersecurity risk assessment that identifies the various information assets that could be affected by a cyber-attack (such as hardware, systems, laptops, customer data, and intellectual property), and then identifies the various risks that could affect those assets. It assists firms in assessing, controlling, and mitigating all types of cyber risks that might affect them. Tunggal (2023) argues that the following are the benefits of performing a cyber risk assessment:

i. Reduction of long-term costs

Identifying and mitigating possible risks and vulnerabilities has the ability to prevent or minimise security incidents, saving your company money and/or reputational damage in the long run.

ii. Provides a cybersecurity risk assessment template for future

When it comes to assessments, cyber risk assessments are one of the practices that need to be updated on a regular basis. A strong first turn of cybersecurity risk assessment ensures repeatable operations even if employee turnover occurs. iii. Better Organisational Knowledge Knowing your company's weaknesses provides you with a comprehensive view of what needs to be improved. Morris (2021) argues that cybersecurity risk assessment can identify potential threats from inside or outside an organisation and the information discovered during risk assessment exposes the drawbacks and limitations of the company current security arrangement and provides an opportunity to fix them.

iv. Avoid Data Breaches

Organisations can suffer a significant financial and reputational loss as a result of a data breach. Hence, it is best to constantly assess risks to find ways to avoid data breaches. Additionally, Morris (2021) suggests that through conducting a cybersecurity risk assessment, a company can identify the entry points that hackers can use to break into systems and create a sound plan for protecting your company and responding to potential assaults.

v. Avoid Regulatory Issues.

Risk assessment ensures that companies comply with regulations of standards like Health Insurance Portability and Accountability Act of 1996 (HIPAA), Payment Card Industry Data Security Standard (PCI DSS), or CPS Australian Prudential Regulation Authority (APRA) 234 to prevent customer data being stolen. HIPAA is an act that sets the standard for sensitive patient data protection. In addition, PCI DSS ensures that firms accept, process, store, and transmit credit card information safely. CPS APRA 234 necessitates that businesses need to improve their information security capabilities in line with the growing magnitude and scope of threats to their assets.

vi. Avoid Application Downtime

For employees and consumers to accomplish their duties, internal or customer-facing systems must be available and functional. Vulnerable systems are easily attacked by malicious actors, which can result in their downtime due to attacks such as Denial of service attack.

vii. Data Loss

Theft of trade secrets, code, or other critical information assets could cost the business. Moreover, data breaches are becoming more frequent these days, so a company can protect

their customers' information by regularly doing a cybersecurity risk assessment, customers will appreciate it; long-term business and increased customer loyalty will benefit you Morris, 2021).

2.6.3 Cybersecurity policies

An IT Security Policy identifies the rules and procedures for all individuals accessing and using an organisation's IT assets and resources and an effective IT Security Policy is a model of the organisation's culture, in which rules and procedures are driven from its employees' approach to their information and work (Palo Alto Networks, 2023). Moreover, policies guide employees on what they should and should not do. A cybersecurity policy lays out how your online systems and software should be used to reduce risk; It enables everyone in the company to comprehend the processes in place to safeguard your firm's data and assets (National Federation of Self Employed and Small Businesses Limited, 2021). The policies ensure the confidentiality, integrity, and availability of the data and assets of the firm. The following topics are the areas that need to be addressed in cybersecurity policies.

i. Acceptable use policy (AUP)

The policy is also known as an Internet Usage and Email Policy or Acceptable IT Use policy. The BioMelbourne Network (2020) argues that in the event of a breach or regulatory audit, an AUP can demonstrate due diligence concerning the security of your IT network and the safeguarding of sensitive data. Organisations use the AUP to create terms and conditions to follow when accessing and operating a business network or internet. Further, Currentware (2023) states that an AUP such as an internet usage policy, work from home policy, or endpoint security policy is an excellent tool for teaching your staff how to use technology in your company, although if they are not adequately enforced, company expectations will be forgotten or ignored. AUP assists in preventing cybersecurity threats, ensuring users are avoiding illegal activities, and focusing on the productivity of employees (Contracts Counsel, Inc., 2023). Email security policies are crucial for promoting pleasant and effective communication while also safeguarding the firm from liability, data loss, downtime, reputational and brand damage, and other issues (Donston-Miller, 2021).

ii. Confidential data policy

InstantSecurityPolicy.com (2022) describes this policy as a policy that identifies what information the company considers "confidential" and specifies how that data should be handled. This policy lays out standards for the use of confidential data and outlines specific security controls to protect this data (The Phoenix Group of Companies, 2023). The policy

covers topics such as access, encryption, and transmission over the network, third-party access, and more.

iii. Mobile device

Helixstorm (2023) argues that without mobile usage standards, companies are left exposed to cybersecurity threats, theft, and corporate espionage attempts. Mobile device policy provides guidelines for using and securing mobile devices within an organisation. Bring your own device (BYOD) policy is an IT policy that permits and assists employees to use personal mobile devices like smartphones, tablets, and laptops to access company data and systems.

With most companies having a BYOD policy for employees, such systems create several issues regarding cybersecurity. It is important to analyse how BYODs can adversely affect a company's information security strategy; BYODs aligned with a company's information security standards allow managers to select what an employee is authorised to do while on the network (Chigada and Daniels, 2021). Hackers can readily access important corporate data if the device runs an outdated or pirated version of the software. The devices make it easier to access your private network if their security is breached. Chigada and Daniels (2021) list compromised data, malware attacks, malicious insiders, shadow IT, absence of BYOD policies, inefficient security control mechanisms and visibility, lack of security awareness, inadequate training, and insecure networks as the security risks caused by BYODs. Furthermore, to mitigate BYOD security risks, making passwords compulsory on all BYOD devices, create a blacklist of prohibited applications, restrict data access, invest in reliable security solutions for devices, backing up device data, and educate employees about security (TechAdvisory.org, 2023).

2.6.4 Incident response policy

The University of Connecticut describes the fundamental objectives of incident response: to limit the scope of an event, minimise the threat to institutional systems and data, and promptly restore impacted systems and data to an operating state. Moreover, Fox (2020) states that in the case of a security breach, an incident response plan ensures that the appropriate individuals and procedures are in place to successfully deal with the attack and allows companies to perform a structured investigation to give a focused response to contain and remediate the threat. In case of any successful breach, organisations need to ensure that data is recovered; there is limited tolerance for downtime that can prevent access to crucial information, as a result, a key component of a data security strategy is making sure that data can be swiftly restored after any loss or damage (Crocetti, 2021). The incident response plan

includes the following six phases: preparation, identification, containment, eradication, recovery, and lessons learned from the attack to prepare for the future.

2.6.5 Network security policy

Rouse (2017) states that a network security policy includes the following: Rules and legal procedures for gaining access to the network and changing its features, web/Internet access governance and management Security measures (access control) implementation on network nodes and devices, and role/privilege-based policies, such as identifying approved and unauthorised network services/processes that every user can execute. The policy largely aids in the protection of a computer network by providing security controls to protect against network security threats posed by the organisation or network, both internal and external. The below figure shows the network security policy lifecycle.

Figure 3: The Network Security Policy lifecycle (Source: Algosec, 2023)

Further, Algosec (2023) argued that a network security policy establishes criteria for computer network access, sets policy enforcement, and outlines the architecture of the organisation's network security environment defines how the security policies are implemented throughout the network architecture.

The following are the network security measures that protect systems and firm assets against cyberattacks (Ochieng, 2023); i. Device security

A company will set up barriers that can only be traversed by certain types of traffic in the form of Private networks, Semi-private networks, and public networks to create effective security for various subdivisions and categories.

ii. Internet access

Access to the internet should be carefully checked and filtered before being used based on the work nature of the user.

iii. VPN policy

Every remote connection to the corporate network should be made using a standard operating system and a VPN that has been approved by the company.

iv. Port communication policy

Ports directly connected to the internet should be limited to or labelled as inbound ports, or only permitted communication services should be used.

v. Wireless LAN policy

To prevent probable wireless network exploitation, an effective network policy should include guidelines on acceptable user authentication, a method for wireless LAN anomaly detection, and a technique for suitable WEP substitution.

vi. Remote connection policy

Only authorised users should have direct access to a company's critical server, while others should have access only through the SSH utility or remote login.

vii. Firewall rules policy

Firewalls may be required at the connection point end to protect communication facilities and private networks.

viii. Intrusion policy

Use Advance Antivirus with inbuilt IPS/IDS to protect against elevated privileges, modified permissions, unauthorised auditing rights, inactive users, registry changes, and more.

ix. Proxy server policy

Proxy servers are often located between a user and a server and are used for both defensive and offensive purposes.

x. Secure communication policy

To defend against attacks, it is recommended to use ciphering techniques like SSH, IPsec, SSL, and TLS, which may virtually encrypt many types of communication including HTTP, IMAP, POP, FTP, and POP3. xi. Demilitarised zone (DMZ) policy

Email servers, databases, web servers, and other systems that require public internet connectivity must be placed on a distinct subnet from the rest of the network.

2.6.6 Password policy

A strong password policy is any company's first line of defence against intruders (Netwrix, 2023). The policy sets of guidelines that provide simple and effective way to protect data and IT systems from unauthorised access through the use of strong passwords. Krishnan (2021) mentions the NIST password guidelines as follows;

i. Minimum length of 8 characters and maximum length of at least 64 characters if chosen by the user.
ii. Allow usage of ASCII characters (including space) and Unicode characters.
iii. Check prospective passwords against a list that contains values known to be commonly used, expected, or compromised.
iv. Limit consecutive failed authentication attempts on a single account to no more than 100.
v. Allow "paste" functionality while entering a password.
vi. No complexity requirements.
vii. No password expiration period.
viii. Enforce multi-factor authentication (MFA).

2.6.7 Physical security policy

Biswas (2020) states that the purpose of the Physical Security Policy is to establish the rules for granting, control, monitoring, and removal of physical access to office premises, to identify sensitive areas within the organisation, and define and restrict access to the same. It provides the framework and guidelines for protecting, managing, controlling, monitoring, and removal the physical resources of an enterprise. According to the cybersecurity experts argue that the three most essential components of a physical security plan are access control, surveillance, and security testing, which work together to make your space more secure (Milkovski, 2021).

Openpath, Inc (2021) describes the four components of physical security controls as firstly Deterrence of unauthorised people from gaining access to company buildings or resources by using access control systems and video security cameras. Secondly, Detection help identifies potential intruder or attack by using alarms, sensors, and automatic notifications. Moreover, Delay can slow down intruders from accessing buildings by using access controls such as key cards or mobile credentials. Lastly, Response controls are used to respond when the breach occurs.

2.6.8 National cybersecurity policy framework (NCPF)

Schultz (2016) states that in South Africa there was a development from common law to The Regulation of Interception of Communications and Provision of Communication-Related Information (RICA) and The Electronic Communications and Transactions (ECT) Acts with regards to cybercrime; the act came into effect in 2005. The objective of the act is to protect the confidentiality of communications, with exceptions limited to serious crimes or threats to national security. Schultz (2016), however, states that the RICA Act is limited in its application and the penalties on the ECT act are not sufficiently strict to stop cybercriminals. All these concerns leave firms vulnerable to the criminals and urges a room for improvement as cyberattacks are increasing in the country.

However, the National Cybersecurity Policy Framework (NCPF) was published in South Africa in 2015 to counter cybercrime, cyber-criminal activity, cyber vandalism, and cyber sabotage (Malatji and Marnewick, 2021). Similarly, Chigada (2021) mentions that the SANCPF was designed to promote the establishment of the National Cybersecurity Advisory Council (NCAC) which oversees the implementation of national cybersecurity strategies and the National Computer Security Incident Response Team (CSRIT). Moreover, the South African government produced the NCPF with the aim of securing public and private infrastructure from cyberattacks. NCPF (2015) states that it provides for measures to counter national cyberspace security; measures to tackle cyber terrorism, cybercrime, and other cyber ills; measures to create, review and amend current substantive and procedural legislation to ensure these align; and measures to build confidence and loyalty in the safe use of ICT.

The framework is implemented with expectations that it will provide a lot of benefits or organisations. It centralises coordination of cybersecurity operations by enabling the establishment of relevant structures, policy frameworks and strategies in support of cybersecurity in order to counter cybercrime, meet national security imperatives and to develop the information society and knowledge-based economy. Also, it Creates cooperation and coordination between the government, the private sector, and civil society by generating and promoting a strong interplay between policy, legislation, societal acceptance, and technology. The framework promotes international cooperation, a culture of cybersecurity, and compliance with appropriate technical and operational cybersecurity standards. Lastly, develops requisite skills, research, and development capacity.

Chigada and Kyobe (2018) state that various pieces of e-legislation intended to combat cybercrime and other computer-related criminal activities have been passed by the South

African Parliament. South African Government (2017) argues that the intent of the offences set out in the Bill which was publicised in 2015 is to protect the confidentiality, integrity and availability of computer data and systems by means of offences of unlawful access, interception of protected data, malware-related offenses, data and computer systems interference and password-related offences. Even though such interventions have been put into place there is still not much change, instead the rate of cyberattacks keep rising. There are still areas of improvements in the policies and regulations to address cyberattacks. Microsoft (2018) states that businesses should keep four services in mind when it comes to successful cloud cybersecurity namely; privacy control and access, data encryption, risk management process, and transparency.

Furthermore, Lotter (2019) argues that for companies to be able to deal with the wide range of threats: firstly, companies must establish a security culture by implementing a multilayered, holistic defence system that involves individuals, policies, and procedures. This helps to ensure that employees understand how and why there is a need to protect the systems, data, and IT assets of the organisation. Secondly, businesses should try to minimise the number of silos to avoid making disparate applications from disparate vendors tacked together haphazardly in an effort to tackle various threats. Lastly, Lotter states that companies should employ a specialist to assist them in lowering IT protection costs by taking a systematic, intelligent approach to security.

2.5.7.1 Protection of Personal Information Act (POPIA)

The research from Deloitte reveals that since people started to work from their homes due to the COVID-19 has highlighted the huge significance of personal data to businesses all across the world, as well as its vulnerability to abuse and attack; cyberattacks rate increased, more especially in the financial institutions. There was an urgency for countries, including South Africa, to re-examine and improve their data privacy and protection legislation in response. In South Africa, the Cybercrimes and Cybersecurity Act and the Protection of Personal Information Act (POPIA) are new laws that will bring the country's data protection and cybersecurity legislation in line with global standards (Baker and McKenzie, 2021). The employment of security safeguards is one of the prerequisites for authorised processing under POPIA. This ensures that the integrity and confidentiality of personal information remains protected. The following are the benefits of the cybercrimes and cybersecurity and POPIA discussed by Williams, Fourie, and Siyaya (2021).

The Act criminalises the disclosure of data messages which are harmful and the disclosure of data messages that contain intimate images and seeks to implement an integrated cybersecurity legislative framework to effectively deal with cybercrimes and address aspects pertaining to cybersecurity. It creates 20 new cybercrime offences and establishes an overarching legal power for dealing with cybercrime by defining how these offenses must be investigated, which includes searching for and acquiring access to, as well as seizing materials related to cybercrime.

Section 3 of the Act defines offences involving personal information (as defined in the POPI Act), such as the abuse, misuse, and possession of another person's or entity's personal information when there is a reasonable suspicion that it was used, or may be used, to conduct a cybercrime. It allows for the establishment of a 24-hour hotline for all cybercrime reporting, as well as the creation of other cybersecurity structures such as a cyber response committee, a cybersecurity centre and a national cybercrime centre. In addition, the act requires electronic communications service providers ("ECSPs") and financial institutions, such as banks, to report cyber offenses within 72 hours of becoming aware of them.

POPIA empowers the South African Police Service to not only investigate, search, access, and seize, but also to collaborate with foreign governments in the investigation of cybercrime. In addition, the Act requires the National Director of Public Prosecutions to submit a report for the National Prosecuting Authority on the number and outcomes of cybercrime prosecutions. The Law also gives South African courts the authority to rule on any act or omission alleged to be a violation of the Act and impacting a person in South Africa, even if the defined cybercrime is committed outside of the country. More importantly, the Act imposes penalties for violators, including fines ranging from R5 million to R10 million and/or imprisonment ranging from 5 to 10 years, with other more serious offences enticing up to 15 years in prison and a maximum sentence of 25 years in prison for computer-related terrorist activity and related offences.

2.6.9 Cybersecurity insurance

The rise in cyberattacks , as well as their broader effects, has prompted insurers and their clients to reconsider the impact on other insurance lines such as personal (reputation), property (physical damage), intellectual property (competitor information), and so on (KPMG, 2018). Cybersecurity insurance was established to reduce losses from cyberattacks , such as data breaches, business disruption, and network damage. Organisations can use cyber insurance to transfer financial risk associated with a cyber incident or attack and cyber insurers

may be well positioned to incentivise better cybersecurity practices since they can reward "good" risk management, provide discounts in exchange for implementing security controls or standards, and provide cybersecurity services that some firms would otherwise struggle to obtain (Maccoll, Nurse, and Sullivan, 2021).

Graham (2021) mentions the following as the events whereby companies can expect to get coverage;

i. Data breach or Distributed Denial of Service (DDOS) attack that brings down your network.
ii. Malware attack that spreads throughout your network's connected devices, rendering it inoperable. iii. Extortion demands made by cybercriminals holding sensitive information they are threatening to expose.
iv. Ransomware demands that lock up devices and threaten to leak sensitive data. v. Business-email compromise resulting in sharing sensitive information.
vi. Liabilities associated with contractual obligations, including within the payment card industry (PCI) Fines and Penalties.
vii. Defending against class-action lawsuits and paying settlements. viii. Legal expenses, fines, and penalties associated with regulatory investigations.
ix. Lost business profits, accrued expenses, and extra costs while actively experiencing a cyber incident, either due to malicious hack or human error.
x. Media liability associated with infringement and other content that is electronically disseminated.
xi. Losses due to social engineering fraud tricking you or your employees into sending funds you should not have.
xii. The business profit lost due to reputational damage to your brand soon following a publicised cyber attack

Additionally, Dataprise (2023) states that cyber insurance cover exclusions include losses due third-party providers protocols, loss of portable devices, war, invasion or terrorism, and security maintenance failures. Due to the increase in cyberattacks and more need for cybersecurity, cyber insurance demand will also go up. However, Palmer (2021) states that the way cyber insurance works will change as the frequency of cyberattacks rises and cyber attackers become more aggressive with their tactics; cyber insurance providers are unlikely to want to provide policies to companies that do not prioritise cybersecurity.

2.7 Chapter summary

This chapter provided a review on the literature of the research pertinent to the topic. As there is a scarcity of study on the subject in South Africa, another literature was evaluated on studies from other countries. The chapter discussed the state of cybercrime both locally and internationally. The various types of cybercrime and the impact they have on the economy were also discussed. Furthermore, cybersecurity as an intervention to combat cybercrime and cybersecurity landscape were discussed. Cybercrime is an on growing issue worldwide, it is significant for companies stay informed and prepare to secure their systems and other assets.

CHAPTER 3
INFORMATION SECURITY STANDARDS

3.1 Introduction

Chapter three focuses on the standards and theoretical framework required in implementing cybersecurity in firms. It commences by firstly discussing the Information Security

Management (ISO/IEC) 27001 then followed by the National Institute of Standards and Technology (NIST). The chapter further discusses the Information Technology Infrastructure Library (ITIL), Control Objectives for Information and Related Technologies (COBIT), Payment Card Industry Data Security Standard (PCI DSS), and CIS Critical Security Controls. Lastly, the chapter presents a summary of the Information Security Standards and concluding remarks.

3.2 Information Security Management (ISO/IEC) 27001

The International Organisation for Standardisation (n.d) states that though there are more than a dozen standards in the ISO/IEC 27000 family, ISO/IEC 27001 is well-known for defining specifications for an information security management system (ISMS). Also, IT Governance (2018) states that ISO/IEC 27001 specifies what an ISMS is required to do; this means that your ISMS must meet these requirements to acquire certification or pass an audit. The standards enable firms to manage the security of assets such as financial information, intellectual property, employee information, and information entrusted by third parties. IT Governance (2021) argues that adopting the standard enables organisations to achieve the information security standards of regulations like the European General Data Protection Regulation (EU GDPR) and the Network and Information Systems Regulations (NIS Regulations). Further, In South Africa, ISO/IEC 27001 certification provides companies operating in the country with the necessary frameworks and tools for improvement of quality, consistency in meeting clients' requirements, and improvement in processes (Business Optimization Training Institute, 2024).

ISO/IEC 27001 is beneficial to organisations since it helps in protecting data. The purpose of the framework of ISO/IEC 27001 is to ensure that there are tools in place to strengthen the firms across the three pillars of cybersecurity (people, processes, and technology); it can help identify the policies needed to codify, the technology you need to defend the company, and the staff training needed to avoid mistakes (Irwin, 2022). The standard reduces information security costs by assisting an organisation in implementing security controls needed and within budget.

In addition, it improves company culture by ensuring that employees are aware of the risks and embrace security as part of working practices. An ISMS encompasses people, processes, and technology, ensuring staff understand risks and adopt security as part of their everyday working practices (IT Governance, 2022). When organisations implement and maintain the

standard, their resilience to cyberattacks improves significantly. Hanna (2022) suggests that the goal of ISO/IEC 27001 is to help organisations protect their critical information assets and comply with applicable legal and regulatory requirements. The framework allows the organisation to be able to respond to evolving security threats. Studies reveal that ISO/IEC 27001 adapts to changes in the threat environment and inside the organisation on a continuous basis, ensuring that information security risks are successfully handled over time. The standard enables the companies to meet contractual obligations regarding factors such as data security. Sahoo (2021) argues that ISO/IEC 27001 encourages the organisation to ensure that they are up-to-date with any documentation, legislation and regulation that affects the achievement of its business objectives and the outcomes of compliance with legal and contractual requirements.

Additionally, Sahoo (2021) argues that ISO/IEC 27001 certification is an essential asset for any organisation working with sensitive data, whether for-profit or non-profit, small business, large business, a state-owned firm, or private sector corporation. Information technology (IT) companies, financial services, telecoms, and any business handling sensitive information must comply with the standard. By serving as an official document that attests to the organisation's high compliance standards and reliable security systems, the certification adds value to the organisation and improves its reputation in the industry, and aids in the avoidance of financial losses or penalties as a result of data breaches or security events.

3.3 National Institute of Standards and Technology (NIST)

The NIST Cybersecurity Framework (NIST CSF) for Improving Critical Infrastructure was first published in February 2014 in response to Presidential Executive Order 13636, "Improving Critical Infrastructure Cybersecurity.". NIST CSF is a voluntary framework designed to help organizations understand, assess, prioritize and communicate about their cybersecurity risks (Morano, 2023). The framework provides recommendations and standards to help companies better prepare for cyberattacks by identifying and detecting them and providing advice on responding to, avoiding, and recovering from them. Similarly, it assists enterprises in managing their cybersecurity risks, incorporating industry standards and best practices.

The National Institute of standards (NIST) states that the framework establishes a common vocabulary that enables employees at all levels of a company and all points in the supply chain to acquire a shared awareness of their cybersecurity threats. Gordon, Loeb, and Zhou (2020) suggest that the NIST framework stipulates that organisation should evaluate their

cybersecurity risk management on a cost-benefit basis; however, it has no direction on how to do such a cost-benefit analysis. The latest releases of NIST are the NISTIR 8170, which provides federal agencies with various options for utilizing the Cybersecurity Framework to tackle prevalent cyber issues. Also, a draft of NISTIR 8286 is the latest release and aims to ensure that cyber risks get the appropriate attention within enterprise risk management programs (Malone, 2020). The framework has three components: core, implementation tiers, and profiles. The Cyber Forum GmbH (2021) states that these components were constructed using existing standards and best security practices from the government and other significant industry sectors.

3.3.1 Components of the NIST framework

i. Core

The core is a collection of desirable cybersecurity operations and outcomes that have been categorised into categories and mapped to informative references. The framework core is intuitive and serves as a translation layer, allowing multidisciplinary teams to communicate using simple, non-technical language; this includes five functions, categories, and subcategories of the framework. The five functions are; **identifying** what needs to be protected, **protection** by implementing a safeguard of the assets, **detecting** the cybersecurity incidents, **responding** by developing techniques to defend against incidents, and **recovering** the service capabilities that were disrupted as a result of the incident.

Vigliarolo (2021) argues that the functions should be considered the organisation's basic incident management tasks. Further, the 108 subcategories are outcome-driven statements that provide ideas for developing or refining a cybersecurity program. The categories were created to cover cyber, physical, and personnel aspects, focusing on business objectives. ii. Implementation tiers.

Bresnahan (2023) argues that the implementation tiers are not intended to constitute a maturity model; instead, they are meant to clarify and guide the relationship between cybersecurity risk management and operational risk management processes. Tiers vary from Partial (Tier 1) to Adaptive (Tier 4) and indicate increasing levels of complexity, how well cybersecurity risk judgments are integrated into broader risk decisions, and the extent to which the company provides and receives cybersecurity information from third parties. Moreover, Clark (2020) states that tier one denotes a business with a reactive, informal approach to cybersecurity risk management, whereas a score of four shows an agile, riskaware organisation with the most sophisticated cybersecurity risk management plan. Tier 1 provides firms with an ad hoc and

responsive cybersecurity posture when protecting data. At tier 2, organisations with a strong understanding of cybersecurity risks may authorise cybersecurity measures, but implementation remains patchy. Further, tier 3 organisations adopt the framework standards across the board and can respond to cyber crises regularly.

Tier 4 is adaptive and signifies firms' complete adoption of the framework.

iii. Profiles

Profiles are the unique alignment of an organisation's organisational goals and objectives, risk appetite, and resources versus the framework core's desired outcomes. According to the National Institute of Standards and Technology (NIST), by constructing a present-state profile, a business can map its cybersecurity requirements, mission objectives, operating procedures, and current practices against the subcategories of the framework core. Comparing current profiles to target profiles helps organisations monitor gaps in their cybersecurity posture and see areas for improvement. Hughes (2022) states that when it comes to attaining goals and decreasing organisational and even industry-wide risk, profiles help provide specific synchronisation with organisation requirements and objectives.

NIST CSF is crucial to fulfil the needs of the United States (US) industry, federal agencies, and the general public. It creates cybersecurity standards, recommendations, best practices, and other tools. Bresnahan (2023) states that the framework provides superior and unbiased cybersecurity; it represents thousands of information security professionals' aggregate experience and is widely regarded as industry best practice and contains the most thorough and detailed set of controls of any framework. NIST framework contributes to long-term cybersecurity and risk management activities. Using this cybersecurity framework will assist your company in identifying and assessing risk, determining which operations are most necessary to crucial service delivery, and prioritising expenditures to maximise the return on your investment (Uzado Compliance and Cybersecurity Services, 2021)

Moreover, the framework builds trust among organisation partners while promoting faster business growth and remaining secure. As the framework allows a risk-based approach to cybersecurity management that is linked with corporate objectives, business and technical stakeholder’s communication and decision-making improves. Halder (2021) argues that compliant firms can use the NIST CSF to stay current and secure at all times; as the framework is adaptable and agile, businesses may align themselves with changing security legislation and future compliance requirements. Lastly, studies show that NIST CSF is designed to meet future regulatory and compliance needs. Bresnahan (2023) argues that it is the most reliable

security measure for building and iterating a cybersecurity program to prepare for new updates to existing standards and regulations.

The NIST CSF affects anyone responsible for making choices about cybersecurity and cybersecurity risks in their enterprises and those in charge of implementing new IT rules (Vigliarolo, 2021). It is used by the government, private and public companies. Illustrated below is an overview of the NIST CSF.

Figure 4: Overview of the NIST Cybersecurity Framework (Source: Researcher, 2023)

3.4 Control Objectives for Information and Related Technologies (COBIT)

Information Systems Audit and Control Association (ISACA) developed the COBIT framework narrow the gap between technical challenges, business risks, and control requirements. Simplilearn Solutions (2023) states that COBIT is a well-known framework that any business may use in any industry, and its strategic approach entails tying company goals to its IT infrastructure by providing multiple maturity models and metrics for measuring progress and outlining business responsibility for IT activities. It is also argued that it helps reduce costs, establish, and maintain privacy standards, and give structure and control to general IT activities within the firm by providing the tools to build, monitor, and enhance its implementation (Shiff, 2021). COBIT is one of the cybersecurity frameworks. It is an excellent umbrella framework for unifying procedures across a complete enterprise as it integrates well with other IT and

cyber risk management frameworks like Information Technology Infrastructure Library (ITIL), Capability Maturity Model Integration (CMMI), and The Open Group Architecture Framework (TOGAF) (Harmony Solutions ltd, 2019). In organisations, the framework ensures information systems are of high quality, controlled, and reliable. In contrast with the primarily IT-centric NIST and ISO/IEC, Wembly Partners (2021) states that the framework specifies the components and design aspects that go into creating and maintaining an overall governance system that is an ideal fit.

ISACA stipulates that COBIT 2019 is an update of COBIT 5; it builds on its solid foundation by incorporating the most recent innovations in enterprise information and technology. Hovarth (2021) states that as COBIT 5 was introduced in 2012, it may not have all of the capabilities necessary to deal with challenges that arise nowadays; risks have evolved, risk management tools and techniques must adapt as well, ensuring that all IT operations are properly prepared to assess, manage, and mitigate all risks while remaining compliant. This framework reinforces the importance of IT governance as a key driver of innovation and business transformation. The updated version addresses cybersecurity and privacy updates, the new data, project, and compliance processes and the links to all applicable standards, guidelines, rules, and best practices have been update. In research, Braga (2020) stipulates that the principles of COBIT 2019 as satisfying stakeholder value, provide a more holistic approach, dynamic governance system, governance distinct from management, tailored to enterprise needs, and end-to-end governance system. Together with the principles the framework uses the seven enablers (people, policies, and frameworks, processes, organisational structures, cultures ethics and behaviour, information, services, infrastructure and applications, people, skills, and competences) to assist firms integrate their IT investments and objectives to maximise the value of those investments.

3.4.1 Elements of COBIT framework

i. Framework

When it comes to IT governance, the COBIT framework is intended to assist enterprises in structuring and classifying all of their goals as well as assists businesses in adhering to IT best practices and integrating them with their overall business needs (Hovarth, 2021). It helps to organise the aims of IT governance and link business requirements ii. Process Descriptions

A process refence model (PRM) is a model that includes descriptions of processes that are specified in terms of their purpose and outcomes, as well as an architecture that describes the links between them. Thomas (2018) identifies this element as the COBIT core model and each of the 40 governance and management objectives in the model relate to a process, which is one of the governance components. It depicts the Plan, Build, Run, and Monitor responsibility areas (PBRM). COBIT framework groups iii. Control Objectives

The framework provides a detailed list of needs for effective IT business management. Control objectives are characterisations of the degree of acceptable results that can be achieved by putting in place control mechanisms for a certain IT process.

iv. Maturity Models

Maturity models are crucial in organisations as the bring more insight on what needs to change to bring companies to the next level by assessing the present level of a team, person, or process. Elue (2020) states that a Capability Maturity Model Integration (CMMI)– based process capability scheme (ranging from 0-5) can be used to help measure the achievement of an enterprise's program and its contribution to the overall enterprise objective; however, using COBIT, which can equally measure the same enterprise program achievements, is done using a concept called "COBIT performance management" (CPM). Further, Elue (2020) argues that the COBIT CPM can help performance management reference how well a company's governance and management system, as well as all of its components, operate together and how they can be enhanced to meet the requisite capacity and maturity levels.

v. Management Guidelines

The management of an organisation uses COBIT guidelines to facilitate the process of assigning of responsibilities and stipulates how COBIT interacts with the organisation as a whole. Hovarth (2021) argues that using COBIT guidelines in the process aids in the creation of a consistent structure throughout the organisation, as well as assisting departments in cooperating and agreeing on their business objectives and measuring overall success.

3.4.2 Governance and Management objectives and processes in COBIT

The framework has governance and management objectives that are grouped into five domains. There is Evaluate, Direct and Monitor (EDM) for governance and Align, Plan and Organise (APO) , Build, Acquire and Implement (BAI), Deliver, Service and Support (DSS), and Monitor, Evaluate and Assess (MEA) for management. Each domain has an identifier that

consists of verbs that express the fundamental goal and areas of action of the objectives they contain. These are discussed as follows:

i. Evaluate, Direct and Monitor (EDM)

The governing body assesses strategic possibilities, guides senior management on the selected strategic options, and monitors the strategy's implementation in this domain (Anoruo, 2019). The domain helps organisations ensure that the objectives are achievable by assessing stakeholder needs; focusing on prioritizing and making decisions, and monitoring performance, compliance, and progress against agreed-upon goals and objectives. Ensured Governance Framework Setting and Maintenance. The processes of EDM include ensured governance framework setting and maintenance, ensured benefits delivery, ensured risk optimisation, ensured stakeholder engagement.

ii. Align, Plan and Organise (APO)

Edmead (2020) states that the domain addresses the overall organisation, strategy and supporting activities for information and technology (IT). APO has the following processes: managed IT management framework, managed strategy, managed enterprise architecture, managed innovation, managed portfolio, managed budget, and costs, managed human resources, managed relationships, Managed Service Agreements, managed suppliers, managed quality, managed risk, managed security, and managed data. The domain emphasises the organisational and infrastructure forms that IT must take in order to achieve the best results and generate the greatest value from its utilisation.

iii. Build, Acquire and Implement (BAI)

Sohail (2023) states that the domain treats the definition, acquisition, and implementation of solutions and their integration into business processes. It encompasses determining IT requirements, acquiring technology, and successfully integrating it into the organisation's present business operations. The processes of BAI include managed programs, managed requirements definition, managed solutions identification and build, managed availability and capacity, managed organisational change, managed IT changes, managed change acceptance and transitioning, managed knowledge, managed assets, managed configuration, and managed projects.

iv. Deliver, Service and Support (DSS)

Anoruo (2019) states that DSS addresses operational delivery and support of IT services, including security. It includes areas of value creation, where IT services add value to the organisation, as well as support activities that make these IT services more effective and efficient. Manage operations, manage service requests and incidents, manage problems, manage continuity, manage security services, and manage organisation process controls are the processes of the domain.

v. Monitor, Evaluate and Assess (MEA)

The domain addresses performance monitoring and conformity of IT to internal performance targets, internal control objectives and external requirements (Anoruo, 2019). The processes of MEA are managed performance and conformance monitoring, managed system of internal control, managed compliance with external requirements, and managed assurance.

COBIT is best for companies as it enhances the IT to assist in achieving objectives. The Business Process Incubator (2020) states that COBIT practitioners are likely to set up the essential controls and tools to assist IT managers in achieving their goals with the full force of their operations behind them and the framework aids firms in establishing measurable IT objectives as part of larger business plans. In simple terms, it aligns with the business and IT goals. Additionally, the COBIT approach focuses on an organisation's values as Its basic model includes a total of 40 Management Objectives and Governance, as well as the CPM which assists organisations in improving their frameworks (Gallager, 2020). It provides enterprises with a management framework that guides them with addressing IT risks and the potential consequences for the firm, business processes, and IT systems. Ellis (2019) argues that since its major role is to allow businesses to be very flexible when developing their governance plans, COBIT can assist a corporation in describing the specific notions of governance and risk management.

Moreover, COBIT is beneficial to organisation as plays well with other frameworks. The framework ensures that firms comply with rules and regulations. The Business Process Incubator (2020) suggests that at all levels of IT management and governance, measures can be used, with strong control and monitoring features in place to guarantee that all criteria are met; this ensures a high level of consistency and allows practitioners to demonstrate their actions in the event of an audit. COBIT promotes the reassessments of IT frameworks to stay alerted with improvements that might be needed. Furthermore, Good e-Learning (2020)

argues because of its focus on framework reassessments and open-source architecture, it also prepares practitioners for future changes. Hence, COBIT is important in organisations.

Kidd (2019) argues that COBIT aids auditors in achieving an acceptable opinion on the rate of assurance on the audited subject matter and provides management with internal control guidance. To ensure effective control, auditors use the flexible concepts, methodologies, processes, and structures for transitioning to change management that are provided by the framework as well as thorough control centric audit checklists and possible evidence gathering sources for ensuring control effectiveness.

In an often unpredictably changing IT environment, managers utilise the COBIT framework to balance risk and investment control.

COBIT principles can be used by enterprise users, usually in-house IT employees, to secure the security and control of IT services offered by internal and external parties (Kidd, 2019). With COBIT, employees and experts stay prepared for all of the worldwide issues that IT processes bring. The figure below summarises the discussion of COBIT principles above:

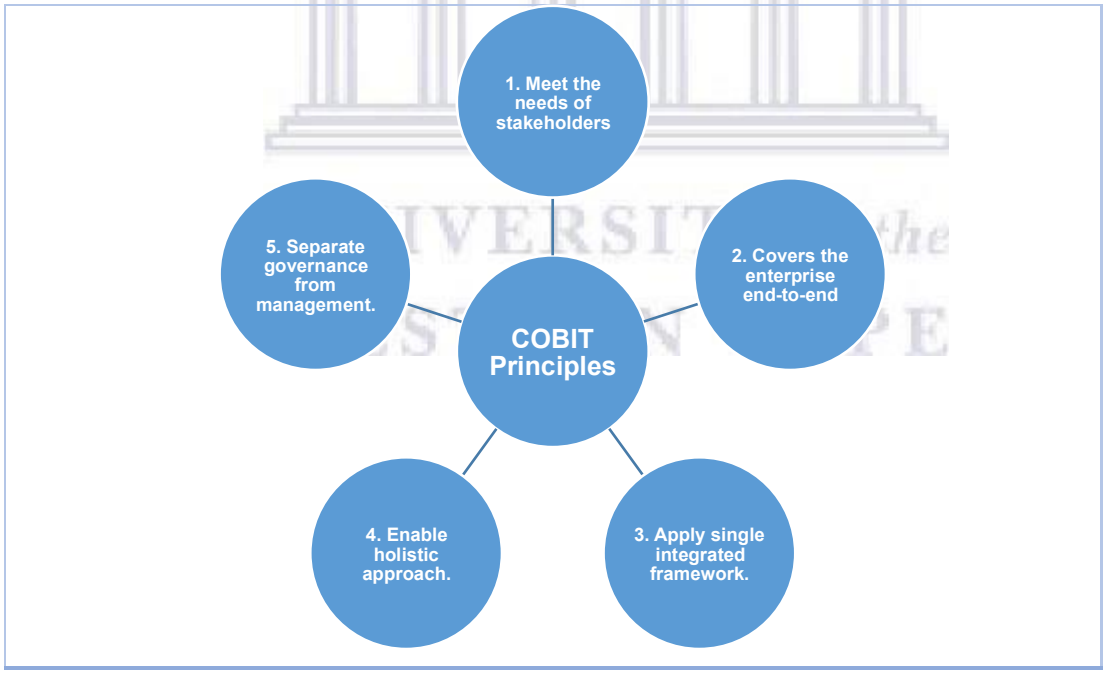


Figure 5: COBIT 5principles (Source: Researcher, 2023)

3.5 Information Technology Infrastructure Library (ITIL)

ITIL aims to help enterprises develop predictable IT systems and provide the best possible customer service to customers and clients by optimizing processes and discovering

possibilities for increased efficiency (White and Greiner, 2022). ITIL framework provides organisations with rules to assist in the developing and managing of IT operations. It does not suggest how to manage changes specifically, but it does recommend some basic best practices, such as categorizing changes by risk and significance and managing them appropriately (Tozzi, 2022). The framework provides specific recommendations to firms, including security. Olcott (2016) argues that the ITIL is more practical for cybersecurity; It is through specific controls that should be in place, like how to handle proper password management and industry-specific compliance requirements that must be met, such as Payment Card Industry (PCI) or Health Insurance Portability and Accountability Act (HIPPA).

Mathenge and Stevens-Hall (2019) states that 4 is the latest version of the framework which allows businesses to co-create meaningful value from IT-supported products and services. ITIL V3 has 26 processes and ITIL V4 offers 34 practices. In addition, ITIL 4's holistic approach elevates the profile of service management in an organisation to a more strategic level, focusing on delivering value, while offering a flexible, coordinated, and integrated system for the effective governance and management of IT-enabled services (Knowledgehut Solutions Private Limited, 2023). The framework focuses on five components, namely, ITIL service value chain, ITIL practices, ITIL guiding principles, Governance, and Continual improvement.

3.5.1 Components of ITIL Service Value System (SVS)

Illustrated in the figure below are the components of the ITIL SVS:

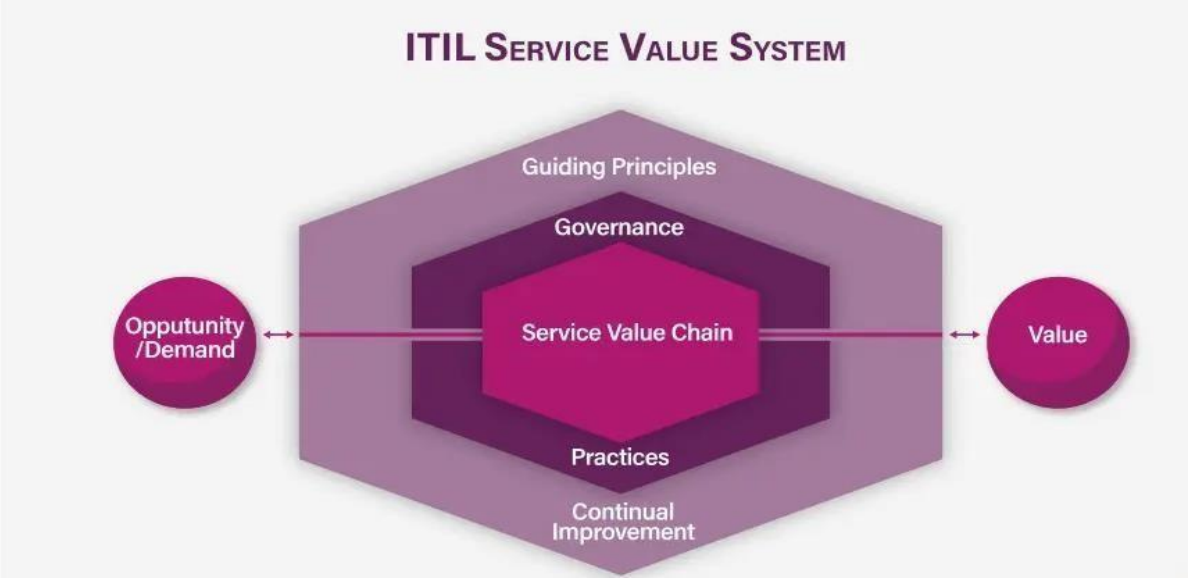


Figure 6: ITIL Service Value System (Source: Axelos, "ITIL Foundation: ITIL 4 Edition", 2019)

I. ITIL Service value chain

Mathenge and Stevens-Hall (2019) define the service value chain component as one that outlines the key activities required to create value in response to demand, through the creation and delivery of products and services. This is the main part of SVS, and studies show that it is versatile enough to be adapted to a variety of approaches such as DevOps and unified IT in order to meet the executives' need for multiple administration models. According to van Bon (2019) it provides an operating model for service providers that covers six key activities, applying practices to continually improve the enabled values. These six activities produce a significant value to organisations by integrating a variety of inputs into specific outputs; they are namely, plan, improve, engage, design and Transition, obtain/build, and deliver and support.

II. ITIL practices

The transition from 'processes' in ITIL v3 to 'practices' in ITIL v4, which recognises that processes are not the only resource to consider; organisations must also consider people, documentation, skills, competencies, tools, partners and suppliers, and so on (IT Governance, 2021). On the IT Governance (2021) green paper, it is discussed that practices allows ITIL to be integrated with other methodologies and the SVS with broader concepts and principles that apply across the organisation. The focus in practices enables entities to create specialised procedures that are tightly matched to the specific needs of its consumers, as well as innovate new processes to embrace modern working methods like Development Operations [DevOps] (Mathenge and StevensHall, 2019).

III. ITIL guiding principles

The ITIL guiding principles give the necessary direction for ensuring shared understanding, developing a standard methodology for service management across the business, and making appropriate organisational decisions and (Knowledgehut Solutions Private Limited, 2023). For example, the direction such as decision-making, collaboration, promotion, values, mission, work, and promotion in the organisation (Yanthan, 2023). The seven ITIL guiding principles, which are the core aspects of the ITIL architecture, are: focus on value, start where you are, progress iteratively with feedback, collaborate and promote visibility, think and work holistically, keep it simple and practical, and optimise and automate. Danby (2023) defines the principles as the recommendations that can guide a company in all circumstances, regardless of changes in its goals, strategies, type of work, or management structure.

IV. Governance

Knowledgehut Solutions Private Limited (2023) states that governance is a formal framework which provides a structure for an organisation to ensure that there is a means for an it to establish direction and control. It lays out the rules, standards, and guidelines that firms can employ to delivery and satisfactory operating.

V. Continual Improvement

Using the ITIL continual improvement model increases the likelihood that IT service management processes will be successful, focuses on customer value, and ensures that improvement efforts are inherently tied to the organisation's vision (AXELOS Limited, 2019). The stage ensures that the effectiveness of services provided to customers. Mathenge and Stevens-Hall (2019) states that this stage is a recurring organisational action carried out at all levels to ensure that the performance exceeds the expectations of its stakeholders.

ITIL is significant and it provides great benefits to the organisations. The framework is advantageous as it ensures that IT and the business are more strategically aligned. Shiff (2021) states that the framework mandates that business and IT targets remain aligned, ensuring that both teams have the same objectives and major goals; this leads to the business as a whole gaining more accountability and clarity, allowing IT teams to provide faster complaint response and release deadlines. Also, ITIL helps with service delivery strategies that are faster and more convenient to enable digital transformation. The service delivery and customer satisfaction improve as a result of adopting the framework in the organisation. The ITIL best practices ensures the seamless functioning of the company's operating systems, allowing customers to have the greatest possible user experience; service-level management helps organisations understand what consumers have come to expect from them so that they can respond appropriately (SolarWinds Worldwide, LLC., 2022).

Moreover, ITIL is beneficial to firms as it gives smoother integration between evolving software delivery practices and the enterprise customer support framework. The framework allows the saving of costs as a result of better resource management. The Lucid Software Inc., (2023) argues that the goal of capacity management is to keep costs low while maintaining a high degree of service quality. ITIL further supports greater transparency of IT costs and assets. Shiff (2021) argues that companies have claimed lower overhead expenses as a result of ITIL, as well as improved visibility into their spending, allowing them to cut out redundant software and other needless service charges. Shiff (2021) states that IT teams can also obtain improved

insights into their spending data through the ITIL's metricbased techniques, which can help them stay on budget and make key decisions when expenses need to be lowered. Lastly, the framework promotes better management of business risk and service disruption or failure. SolarWinds Worldwide, LLC. (2022) Change, incident, and issue management processes in ITIL are aimed at preventing service outages and swiftly resolving them when they do occur and with the benefits of using ITIL risks are managed.

ITIL is used by organisations to improve their service value; these include small, medium, and large entities. The framework is widely adopted by companies but includes focus on the customers, suppliers, managers, and employees.

3.6 Payment Card Industry Data Security Standard (PCI DSS)

Card fraud remains to be an issue in South Africa and the rest of the world. South African financial firms and other firms that deal with card transactions are required to comply with the PCI standard. Chigada (2020) states that in response to the rise in cybercrimes, the Payment Association of South Africa (PASA) was urged to adopt zero-floor limits for all merchants and stop issuance of nonchip or Personal Identifiable Number (PIN) credit cards. Suggestions have been made to adopt more robust security solutions that enhance confidence of the banking clientele, industry, and economy as a whole.

This is a cybersecurity standard and is enforced by the payment card industry security standards council. The PCI DSS Council's purpose is to improve worldwide payment account data security by creating standards and supporting services that encourage stakeholder education, awareness, and effective implementation. Baykara (2020) states that version 4 of the standard has been released and it replaces version 3.2.1 to address emerging threats and technologies better and provide innovative ways to combat new threats. The latest version intends to address the payment industry's increasing security needs, promote security as a continuous process, expand agility, and improve procedures for businesses utilising various ways to achieve security goals.

PCI DSS applies to all companies that store, process, or transmit cardholder data (CHD) and/or sensitive authentication data (SAD) or have the potential to compromise the security of cardholder data (CDE); This comprises of merchants, processors, acquirers, issuers, and other service providers who are involved in payment card account processing (Payment Card Industry Security Standards Council, 2018). The PCI DSS is a collection of policies and

procedures developed to improve the security of credit, debit, and cash card transactions and protect cardholders from identity theft. There are twelve requirements for PCI DSS compliance. The Reciprocity (2023) argues that payment card industry (PCI) requirements define the physical access, anti-virus software, security systems, public networks, and network resource controls necessary to maintain compliance. Failure to meet all the standard requirements results to fines and the suspension of an organisation's right to accept or process card transactions. Fruhlinger (2022) states that organisations should determine PCI DSS level based on how many credit card transactions they handle in a year, complete the standard compliance checklist, build secure network, and formally attest compliance within the organisation to ensure compliance with the standard. In level 1 of PCI DSS businesses process over 6 million card transactions annually, 1 to 6 million card transactions are processed in level 2, 20000 to 1 million transactions are handled in level 3, and lastly, less than 20000 transactions are processed annually. Additionally, Coos (2019) suggests that data transparency, securing your data on the move using tokenisation and encryption, restrict data access rights, training of employees, and documenting and logging everything are the best practices to ensure compliance.

3.6.1 Requirements for PCI DSS

i. Install and maintain a firewall configuration to protect cardholder data

Firewalls are significant as they prevent unauthorised access to sensitive data. Rane (2022) states that this requirement ensures that service providers and merchants maintain a secure network through the proper configuration of a firewall as well as routers if applicable.

ii. Do not use vendor-supplied defaults for system passwords and other security parameters

Compliance with securing devices and software with valid passwords is vital as it protects them from being easily accessed by the public. Exabeam (2022) suggests that to comply with PCI, firms must develop an inventory of all devices affecting the cardholder environment and confirm they all have secure passwords and appropriate security settings.

iii. Protect stored cardholder data

The Vicente (2023) contends that requirement 3 stipulates that, unless it is absolutely necessary for business function, cardholder data should not be stored at all. Card data encryptions are implemented using encryption keys, and they are also required to be encrypted for compliance.

iv. Encrypt transmission of cardholder data across open, public networks

When the cardholder data is transferred to known destinations, it must be encrypted, and account numbers should never be transmitted to unidentified locations. Encrypting cardholder data before transmitting it using a secure version of transmission protocols like TLS, SSH, and others can help reduce the chances of it being exploited (Rane, 2022).

v. Use and regularly update anti-virus software or programs

Outside of PCI DSS compliance, installing anti-virus software is a recommended practice that must be patched and updated regularly. It is essential that where anti-virus cannot be implemented directly, one's POS provider should use anti-virus measures. Glover (2023) states that maintaining an up-to-date anti-malware program will prevent known malware from infecting systems.

vi. Develop and maintain secure systems and applications

All software on devices that interact with or store cardholder data, in particular, need updates that include security measures such as patches to address newly discovered vulnerabilities, which adds another layer of protection. The Vicente (2023) suggests that PCI DSS requirement 6 has become increasingly critical in light of recent major data breaches to code like Log4J; even code created to maintain audit logs must be safeguarded, access to the code must be limited, and software engineers must be trained in secure coding practices.

vii. Restrict cardholder data access.

The PCI DSS mandates that roles that need sensitive data must be well-documented and updated regularly. To fulfil requirement 7, organisations need a role-based access control (RBAC) system, which grants access to card data and systems on a need-to-know basis (Glover, 2023). viii. Assign a unique ID to each person with computer access.

Individual credentials and identity should be required for access to cardholder data. Unique IDs reduce susceptibility and speed up response time if data is compromised. This requirement does not only defend against illegal data access, but also allow investigators to determine whether or not an authorised insider mishandled data (Fruhlinger, 2022).

ix. Restrict physical access to cardholder data.

Data that is physically written, as well as data that is stored digitally, should be kept in a secure location. Requirement 9 covers the measures that vendors must take to secure the physical environment in which card payments may be accepted, and where cardholder data may be transmitted or stored (Vicente, 2023).

x. Track and monitor all access to network resources and cardholder data. Document how data flows into the company and the number of times access are required to ensure compliance. To verify the accuracy, software solutions to log access are also

necessary. Additionally, obtaining system logs, according to Sanchez (2021), assists companies in tracking user activity and is crucial in preventing, identifying, or mitigating the impact of a data security incident.

xi. Regularly test security systems and processes.

Fulfilling the PCI DSS requirement through regular scans and vulnerability testing helps limit threats against the organisation. Rane (2022) states that on a quarterly basis, internal vulnerability scan, all external IPs and domains exposed in the CDE must be scanned by a PCI Approved Scanning Vendor (ASV) and a wireless analyser scan must be performed to detect and identify all approved and illegitimate wireless access points. Further, at least once a year, or after any significant change, all external IPs and domains must go through a comprehensive application and network penetration test as well conduct file monitoring weekly.

xii. Maintain a policy that addresses information security for employees and contractors. For compliance, an inventory of equipment, software, and employees with access will be required. Moreover, the logs of cardholder data, how information enters an organisation, where it is stored, and how it is used after the point of sale must be documented. Glover

(2023) suggests that the annual, formal risk assessment that identifies essential assets, threats, and vulnerabilities is the second element of requirement 12; it assists firms in identifying, prioritizing, and managing your data security concerns.

3.6.2 Benefits of PCI DSS

The primary factors when implementing an IT infrastructure are data compliance and management, particularly the processing and store sensitive consumer data. In organisations, complying with PCI DSS helps with preventing data breaches. When businesses adhere with its requirements, including that of putting up firewalls, encrypting data, and implementing an information security management system, they are addressing the most common vulnerabilities that attackers target (Irwin, 2021). The standard provides measures that enable organisations to reduce possibilities of cyberattacks as well as ensuring safety during data related incidents. Consumers have confidence in businesses that are well-protected against security breaches. Vumetric Cybersecurity Inc. (2023) claims that being PCI compliant provides companies an advantage over competitors who are not, maximises the sales potential, and helps establish client trust, resulting in more returning customers.

In addition to the benefits, complying with PCI DSS allow businesses to meet global standards. The SysGroup (2022) state that achieving PCI compliance allows companies to join the ranks of other global merchants and enterprises dedicated to data security and consumer protection. The standard prioritises security by enforcing that organisation utilise numerous levels of security and provides IT security procedures that are flexible to new threats and monitors network for unpatched holes or out-of-date software. Goodspeed (2022) describe PCI DSS as a global standard that provides a baseline of technical and operational requirements designed to protect account data.

3.7 Center for Internet Security (CIS) Critical Security Controls

The SANS Institute (2021) states that the CIS Controls (formerly known as Critical Security Controls) is a recommended set of actions for cyber defence that provide specific and actionable ways to stop today's most pervasive and dangerous attacks. There are 18 controls in the newly improved version 8 of CIS controls as described by the Center for Internet Security, they are as follows:

3.7.1 Inventory and control of enterprise assets

Schrader (2023) states that the CIS asset management control provides information that can help enterprises identify the critical data, devices and other IT assets in your network and control access to them. This control actively manages all enterprise assets such as end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers that are connected to the infrastructure physically, virtually, remotely, and in cloud environments, to accurately know the totality of assets that need to be monitored and protected within the enterprise. It further assists in detecting unlawful and unmanaged assets that need to be removed or repaired.

3.7.2 Inventory and control of software assets

The control help organisations to actively manage all software (operating systems and applications) on the network to ensure that only authorised software is installed and may execute, and that unauthorised and unmanaged software is identified and stopped from being installed or running. It ensures only authorised software is used by the firms will increase the effectiveness of risk management efforts and allows companies to quickly identify unauthorised and unmanaged software can prevent security breaches and increase the productivity of users (Tenable, Inc., 2023).

3.7.3 Data protection

The control helps by providing proposed methods and technical controls to identify, classify, securely handle, retain, and dispose of data. For example, the Center for Internet Security (2021) states that it is important for an enterprise to develop a data management process that includes a data management framework, data classification guidelines, and requirements for protection, handling, retention, and disposal of data; this control helps firms with these strategies.

3.7.4 Secure configuration of enterprise assets and software

For cybersecurity, compliance, and business continuity, it is vital to keep all of IT assets configured securely as even a single setup error might result in security breaches and business interruptions (Schrader, 2023). The control is used to establish and maintain secure configurations for organisational resources such as portable and mobile end-user devices, network devices, non-computing/IoT devices, servers, and software (operating systems and applications).

3.7.5 Account management

In organisations, knowing who has credentials, how those credentials are granted, and how they are being used is the foundation of any secure environment (Wenning, 2021). The control helps firms in assigning and managing authorisation to credentials for user accounts, including administrator and service accounts, to firm assets and software using processes and tools.

3.7.6 Access control management

The control provides processes and tools to create, assign, manage, and deactivate access credentials and privileges for a user, administrator, and service accounts for enterprise assets and software. In an organisation, this control is implemented to control what access the user accounts have by focusing on ensuring that users have only access to the data or assets that are in line with their positions and ensuring that sensitive company data or operations are protected using strong authentication becomes easy.

3.7.7 Continuous vulnerability management

Vendors, for instance, are required to develop and deploy patches, indications of compromise (IOCs), and upgrades whenever researchers or the community disclose new vulnerabilities; defenders must evaluate the enterprise's risk from the new vulnerability, regression-test patches, and apply the patch (Release Stable, 2022). This control helps cybersecurity

professionals to develop a strategy for constantly evaluating and monitoring vulnerabilities across the company's infrastructure to remediate and reduce the window of opportunity for attackers. Also, it helps to keep track of new threat and vulnerability information from public and private industry sources.

3.7.8 Audit log management

The purpose of this control is to gather, alert, evaluate, and keep audit logs of events that could aid in the detection, understanding, or recovery from an attack. Reguly (2021) argues that all businesses with enterprise assets should implement the Control and it is made up of twelve safeguards, most of which are in the IG2 category and have Protect or Detect security functions. Further, audit logs should include precise information regarding (1) the event, (2) the system on which the event occurred, (3) the time the incident occurred, and (4) the person who caused the event to occur (Reguly, 2021).

3.7.9 Email web browser and protections

A successful social engineering attack through emails and web browsers could give an attacker an entry point within an organisation (Swoboda, 2021). The control assists in enhancing email and online threat safeguards and detections; these allow attackers to control human behaviour through direct involvement.

3.7.10 Malware defenses

The Release Stable (2022) argues that malicious software (sometimes categorised as viruses or trojans) is an integral and dangerous aspect of internet threats and can serve a variety of functions, such as capturing credentials, stealing data, identifying other targets within the network, and encrypting or destroying data. Malware defense control serves as a reminder that this technology is as critical as it ever was and lays out the minimum requirements for ensuring your malware defences are up to the task (Reguly, 2021). It prevents or restrict malicious applications, code, or scripts from being installed, disseminated, or executed on assets of the company.

3.7.11 Data recovery

Wenning (2021) states that firms should be able to recover data in an event of data loss but should also be able to recover if company losses data integrity which may be the case after a security breach with unknown impacts on the system. The control aims to develop and sustain

data recovery procedures that will allow in-scope enterprise assets to be restored to their pre incident, trusted status.

3.7.12 Network infrastructure management

Network Infrastructure management control helps in initiating, implementing, and actively managing network devices to prevent attackers from exploiting weak network services and access points. This control provides ways to manage the network infrastructure such as the appropriate security architecture, addressing vulnerabilities that are, often times, introduced with default settings, monitoring for changes, and reassessment of current configurations (Center for Internet Security, 2021).

3.7.13 Network monitoring and defence

The control establishes and maintains comprehensive network monitoring and defence against security threats throughout the enterprise's network architecture and user base using processes and tools. Organisations should have people, processes, and technologies in place for monitoring, detecting, logging, and preventing malicious activities that occur when an enterprise experiences an attack within or against their networks (Thames, 2021).

3.7.14 Security awareness and skills training

Users that lack the necessary security awareness training are regarded a weak link in an organisation's security as they are easier to exploit than finding a flaw or vulnerability in the equipment that an enterprise uses to secure its network (Swoboda, 2021). The control help establishes and maintain a security awareness program to encourage employees to be security-conscious and well-trained to lessen the company's cybersecurity risks. The awareness provides information on effective security practices such as ways to not mishandle sensitive data, how to note phishing emails, and setting strong passwords.

3.7.15 Service provider management

Jerzewski (2022) states that because some businesses rely on third-party infrastructure for day-to-day operations, it is critical to understand the legislation and security requirements that a service provider promises to follow. The control's main aim is to assist in developing a strategy for evaluating service providers who handle sensitive data or are in charge of an organisation's essential IT platforms or processes to verify that those platforms and data are properly protected. This control in the organisation provide ways in which third parties can be managed and monitored to reduce the risks.

3.7.16 Application software security

The control is used to manage the security life cycle of in-house designed, hosted, or purchased software to avoid, detect, and correct vulnerabilities before they harm the company. Rather than navigating a labyrinth of networks and systems, today's attackers see an opportunity to exploit an organisation's applications to circumvent network security safeguards and compromise important data (Jerzewski, 2022).

3.7.17 Incident response management

Incident Response Management control help organisations to establish a program to prepare, detect and respond rapidly to an attack by developing and maintaining an incident response capacity. If an enterprise is neither equipped nor prepared for that potential data breach, they are not likely to succeeded in responding to the threat (Reguly, 2022).

3.7.18 Penetration Testing

Firms use this control to identify and exploit weaknesses in their controls and replicate the objectives and behaviours of an attacker to test the effectiveness and resiliency of business assets. For example, in a firm a penetration testing takes these flaws a step further by trying to exploit them to discover how far an attacker could penetrate and what data or business processes might be affected (Center for Internet Security, 2021).

3.8 Chapter Summary

Chapter three provided an insight to different standards and frameworks that enterprises should comply to in order to implement and maintain good cybersecurity. The researcher first discussed ISO/IEC 27001 and followed by NIST CSF and it components. Additionally, COBIT was discussed as well as its elements and governance and management objectives and processes. The chapter then outlined ITIL and its components. Further, PCI DSS, its requirements and benefits were discussed. Lastly, the chapter presented and described the 18 CIS Critical Security Controls.

CHAPTER 4
RESEARCH DESIGN AND METHODOLOGY

4.1 Introduction

This chapter focuses on discussing the research design and methodology which was followed in this study. The chapter provides an in-depth view of research paradigm, research design research Method, target population, instrument development, sampling techniques, pilot study, data Analysis, thematic data analysis , and trustworthiness the of the study. It further presents ethical considerations of the study and the summary of the chapter.

4.2 Research paradigm

A paradigm is a specific theoretical orientation, based on a particular epistemology and research methodology, reflective of a particular scientific community at a particular time in

history (Geskey *et al*., 2012). Additionally, Lecturer (2018) defines a paradigm as the set of common beliefs and agreements shared between scientist about how problems should be understood and addressed. The scientists influence the type of theory that is developed for a broad audience. Research paradigms include positivism, critical theory, realism, and interpretivism. Firstly, Park, Lars, and Artino (2019) refer to positivism as a paradigm which relies on the hypothetico-deductive method to verify existing hypothesis that are frequently articulated quantitatively, where functional correlations may be derived between causative and explanatory factors (independent variables) and outcomes (dependent variables). The positivist paradigm is not only used in quantitative studies but can be used in qualitative studies too. Additionally, from an epistemological point of view, positivist qualitative research focuses on looking for patterns and causal linkages between various aspects of reality using non-statistical methods, then synthesizing those patterns into broad conclusions (Su, 2018).

According to Froner (2018), the critical paradigm places social justice issues at the center of its study and aims to address the political, social, and economic problems that underlie social injustice, conflict, struggle, and power systems at all possible scales. Critical theory is frequently referred to as the transformative paradigm since it aims to alter politics in order to address social oppression and enhance social justice in the particular situation (Froner, 2018). The third paradigm is realism paradigm and as defined by Eastwood *et al.* (2018), it is the view that entities exist independently of our perception or our theories about them. There is a direct realism and critical realism group. To differentiate between the two groups, Dudovskiy (2022) argues that direct realists acknowledge that the world is relatively steady, and on the other hand, critical realists recognise the significance of multilevel research. Moreover, Putnam and Banghart (2017) states that Interpretive methods include social theories and viewpoints that support the idea that reality is socially produced or given meaning by how actors interpret occurrences. With the discussed four paradigms above, Yong et al. (2021) further differentiate paradigms as follows; positivism is used for quantitative research, while the other three are used in qualitative research. The authors state that critical theory researchers aim at critiquing and transforming social, political, cultural, economic, ethnic and gender values. Furthermore, Yong et al. (2021) argue that realism believes that there is a “real” world to discover even though it is only imperfectly apprehensible and that interpretivism enquires about the ideologies and values that lie behind a finding so that reality consists of “multiple realities” that people have in their minds.

The study employed an interpretivist research philosophy as this view supports a qualitative method for data collection. Dudovskiy (2022) states that the primary data obtained in interpretivist studies cannot be generalised since personal viewpoints and values have a significant impact on the data; as a result, data representativeness and reliability are also slightly undermined. On the contrary, the primary data generated through interpretivism studies might be associated with a high level of validity because data in such studies tends to be trustworthy and honest (Dudovskiy, 2022). Above all, this research paradigm was used in the study because it allowed the researcher to examine, explain, express, and try to put themselves in the participant's mindset in order to reconstruct the statement's intended meaning during the analysis of the data collected. Through this approach, the information was gathered through narrative interviews in an effort to be more or less subjective; the people have amassed experiences, opinions, and attitudes in favourable situations and are supported by certain value structures of their culture and society (Pervin and Mokhtar, 2022).

4.3 Research design

Boru (2018) defines research design as the long view strategy for binding conceptual research issues to relevant (and feasible) empirical research. Similarly, Akhtar (2016) argues that research design can be thought of as the framework for research; it is the "Glue" that binds all of a research project's components, in other words, it is a proposal for the planned research work. The selection of the research method, which defines how relevant information for a study will be collected, is a key decision in the research design process (Sileyew, 2020). A research design in a qualitative study can be descriptive, correlational, experimental, diagnostic research and exploratory design. Firstly, descriptive research aims to provide the most precise description of the phenomena that already exist. For example, *"One can conduct a descriptive study about the employees at a factory, their age distribution, community-wise distribution, level of education, state of their physical health, and so forth.*
One can also study the conditions of work in a factory, including health, safety, and welfare.", Akhtar (2016).

Secondly, Bhandari (2021) states that a correlational research design investigates relationships between variables without the researcher controlling or manipulating any of them. Thirdly, experimental design is a scientific method of conducting research in which one or more independent variables are altered and applied to one or more dependent variables in order to determine their influence on the latter (Zubair, 2023). Additionally, the phrase "existing phenomena" on descriptive research distinguishes it from experiment research, which also

detects phenomena after a specific period of treatment and that he findings of descriptive research have already been made available (Atmowardoyo, 2018). The fourth research design is diagnostic research and researchers use it to assess how frequently something occurs and how it interacts with other factors. Ansari *et al.* (2022) argues that,

> *"Diagnostic research design includes the inception, diagnosis and solution for the issue, Inception of the issue asks that, when did the issue arise? In what situations is inception issue more evident? Diagnosis of the issue states, what is the underlying cause of the issue? What is influencing the issue to worsen? Solution for the issue is to tell about what is working in curing the issue? Under what situations does the problem seem to become less evident?".*

The fifth research design is the exploratory and was adopted by the researcher in this study. The researcher used exploratory design to familiarise themselves with an existing phenomenon of information system security in financial firms and gain new insight into it in order to define a more specific problem. Ansari *et al.* (2022) states that explanatory research design always starts with a theory or hypothesis and after gathering evidence it approves or disapproves a theory. Exploratory research can lead a researcher to the right direction towards what the answer is; however, it uses a smaller sample size, it is not possible to appropriately interpret the findings for a broader population (Bhat, 2024). Even so, the exploratory research design enables the researcher lay a solid basis for exploring ideas, selecting the most appropriate study design, and identifying variables that are truly crucial for a thorough analysis (Bhat, 2024). Hence, the research's findings were then used to identify issues that are pertinent to the study's topic. With many aspects of cybersecurity, the study's predominant design were interviews which were be supplemented by case studies of previous security incidents in South African financial institution. The interviews gave the researcher meaningful insight that a generalised public source could not be able to provide.

4.4 Research methodology

This study employed a qualitative dimension which demonstrated the social and human aspect to cybersecurity. The three main methodologies often employed in research are quantitative, qualitative, and mixed methods approach. The comprehensive study of phenomena through the gathering of numerical data and use of mathematical, statistical, or computational methods is known as quantitative research (Adedoyin, 2020). Quantitative research methodology is employed when the data being gathered is quantifiable. In a quantitative study, data is

collected using surveys which contains close-ended questions. Secondly, Bhandari (2022) describes qualitative research as a method that involves collecting and analysing nonnumerical data to understand concepts, opinions, or experiences and can be used to gather in-depth insights into a problem or generate new ideas for research. The collection and analysis of non-numerical data of a qualitative method helps researchers comprehend ideas, opinions, or experiences to gain the insights. Data is collected through observations, interviews, focus groups, surveys with open-ended questions, and secondary research. To differentiate the two methods, Cibangu (2012) refers to quantitative researchers as researchers that disconnect themselves from the real world in order to manipulate and study the selected phenomenon and qualitative researchers as researchers who seek out and immerse themselves into the real, uncontrolled, crude, and non-manipulated world (of humans) to derive and interpret the hidden patterns (theories). Further, when a researcher uses a mixed method approach, that means the data of the study there both quantitative and qualitative data collected and analysed for that study. The researcher of this study adopted a qualitative method. Mwita (2022) argues that in qualitative research it is challenging to achieve one of the important aspects of research, which is the ability of the research findings to produce similar results under the same methods and under similar circumstances. However, it was important for the researcher to get a better comprehension of experiences, occurrences, and context of information system vulnerabilities in financial institutions to find answers to research question, hence the use of qualitative research. The method is flexible and allowed the researcher to collect as much data as possible based on the participant experiences.

4.5 Target population

The study population should be specified in all experimental, observational, and qualitative research involving human subjects in order to ascertain who is qualified to participate in a study (Eldredge, Weagel and Kroth, 2014). To ensure the overall validity of the study results, the population of the study should be defined precisely. Asiamah, Mensah, and OtengAbayie (2017)The target population is determined using selection criteria to select individuals of the general population who can, at best, share experiences and thoughts under the most convenient conditions. The target population of this study was the cybersecurity professionals from Cape Town financial firms.

4.6 Instrument development

For this study, semi-structured interviews were used as the primary data collection instruments. The information was gathered from 8 participants to gain their personal experiences and perspectives on events at the financial institutions interviewed. Interviews enabled respondents to provide full insights on the security implications faced by the financial firms. Semi-structured interviews frequently have an open-ended format that promotes flexibility and a sense of order while adhering to a specified theme framework; they are frequently referred to as having "the best of both worlds" because of this (George, 2022). The researcher constructed open-ended questions for interviews in such a way that the responses addressed the main research question as well as the sub-questions. The table below will demonstrate the link between research questions and interview questions is illustrated in

Interview question(s)	Main focus areas	Research question
1, 2, and 6	Cybercrime	What is the current state of cybercrimes in South African financial sector?
7	Readiness to address cybercrime	How prepared are the financial institutions to address cybercrimes?
3, 4, 5	Investment in Cybersecurity	To what extent do South African financial institutions invest in information systems security? What challenges are faced by South African financial institutions when implementing cybersecurity strategies?
9	Improving cybersecurity controls	How can firms improve their information systems security controls in order to reduce information systems security vulnerabilities?

Table 1: The link between research questions and interview questions (Source: Researcher, 2023)

These questions (see appendix 1) assisted the researcher while gathering the qualitative data from the respondents. A total number of 7 firms agreed to conduct the interviews for collecting data and the semi-structured interviews were conducted through online interviews with 8 participants. Additionally, interviews were facilitated by the researcher on Microsoft Teams and were recorded and transcribed for data analysis.

4.7 Sampling techniques

Sampling can be defined as the method or the technique consisting of selection for the study of the so-called part or the portion or the sample, with a view to draw conclusions or solutions about the universe or the population (Singh, 2019). It is rarely possible to gather data from every member of a group of individuals when conducting research on them, hence researchers select a sample (McCombes, 2019). The sampling method is used by the researcher to choose a sample that represents the population in all the respects. The 2 types include probability and non-probability sampling. Bhardwaj (2019) states that each member of the population has a known probability of being chosen for the sample in probability sampling. Simple random sampling, cluster sampling, systematic sampling, and stratified random sampling are the types of probability sampling techniques. Firstly, Thomas (2023) describes the simple random sampling, compared to other probability sampling techniques, as the easiest one to understand because it only needs one random selection and little prior population knowledge; each participant in a population has an equal chance to be selected.

In a cluster sampling, the population of the research is grouped into smaller clusters and participants are randomly selected. Thomas (2023) argues that large populations, especially those that are widely geographically distributed, are frequently studied using cluster sampling technique. Thirdly, Hayes (2022) refers to systematic sampling as a type of probability sampling technique in which sample participants are chosen from a broader population using a random starting point but with a predetermined, regular interval. The fourth probability sampling, known as stratified random sampling, is discussed by McCombes (2019) as the sampling technique that includes segmenting the population into smaller groups that might have significant differences and by ensuring that each subgroup is fairly represented in the sample, it enables a researcher to reach more accurate findings. The

In this study, the researcher adopted a non-probability sampling technique. Etikan and Bala (2017) describe non-probability sampling as a sampling method that does not provide any basis for a probability estimate that components from the universe will be included in the study sample. When using this technique, rather than random selection, samples are chosen depending on the researcher's subjective evaluation. The different types of sampling techniques considering the non-probability designs include convenience sampling, quota sampling, purposive sampling, self-selection (volunteer) sampling, and snowball sampling. Bhardwaj (2019) describes the sampling techniques, *"In purposive sampling participants are chosen based on the purpose of the study, convenience sampling involves selecting the*

members of a sample on the basis of their convenient accessibility is called convenience sampling. In quota sampling, participants are selected on the basis of some specific characteristics chosen by the researcher.". Additionally, Nikolopoulou (2022) argues that the self-selection sampling (also called volunteer sampling) relies on participants who voluntarily agree to be part of your research.

Moreover, the fifth non-probability technique, which was in this study, is the snowball sampling. Babbie (2010) states that the snowball sampling is often employed in field research to find out whereby each person may be asked to suggest additional people for interviewing. Heath (2023) points out that as participants tend to refer people they know in snowball sampling, researchers run the risk of sample bias. Even so, the sample was still appropriate for the study as the firms would best know the cybersecurity employees that can be part of the study. A total number of 7 firms agreed to participate in the interviews for collecting data. The interviews were conducted using an online platform, Microsoft Teams. There was a total of 8 participants for the study; one financial firm agreed that the researcher interviews 2 participants and 6 other firms agreed to one participant each. For this data collection, the researcher approached different financial firms (see Appendix 5) and the sample was based on the financial firms that provided feedback and agreed to participate. Participants for this study were only disclosed when approaching firms for is because at the beginning of the research, people who were involved in reacting to and investigating previous cybersecurity breaches within the firms were not known.

4.8 Pilot study

Crossman (2019) states that a pilot study is a preliminary small-scale study that researchers conduct in order to help them decide how best to conduct a large-scale research project. Additionally, a pilot study provides the data required to determine the sample size and to evaluate all other components of the primary study, reducing the need for extra work from the researchers and participants as well as the waste of research resources (In, 2017). The number of interviews conducted for the research was 8. Studies suggests that a pilot study sample should be 10% of the sample size planned for the final study (Ismail, Kinchin, and Edwards, 2017). The sample of the study was 8 participants and the pilot interviews for this study were conducted with 2 participants. With the use of pilot study, the researcher was able to calculate the amount of time and resources needed to finish the research. The researcher

used the pilot study data collection as proposed data collection method on a larger population, in order to ensure that the preferred data collection method will suffice on larger populations.

4.9 Data analysis

Qualitative data analysis is concerned with transforming raw data by searching, evaluating, recognising, coding, mapping, exploring and describing patterns, trends, themes and categories in the raw data, in order to interpret them and provide their underlying meanings (Ngulube, 2015). In qualitative analysis, Flick (2014) suggests that whatever the data are, it is their analysis that, in a decisive way, forms the outcomes of the research.

4.9.1 Thematic data analysis

Thematic analysis was used in analysing the data. Thematic analysis is an analysis method that entails searching across a data set to identify, analyse, and report repeated patterns (Kiger and Varpio, 2020). Thematic analysis is more accessible to researchers and Nowell *et al.*, (2017) states that it is effective in summarising significant elements of a huge data set, as it forces the researcher to take a well-structured approach to handling data, helping to produce a clear and organized final report. The goal of a thematic analysis as stated by Maguire and Delahunt (2017) is to identify themes, i.e., patterns in the data that are important or interesting, and use these themes to address the research or say something about an issue. For this study, the researcher followed the six phased presented above with the analysis of data. The below figure illustrates the six phases of thematic analysis by Braun and Clarke (2006).

Figure 7: Six phases of thematic analysis (Source: Researcher, 2023)

After the interviews were conducted with the participants, the above steps were followed to analyse the data. To familiarise themselves with the data, the researcher transcribed the interviews, then organised and searched for these to generate codes. Moreover, the

researcher reviewed the data to identify patterns data coding and see if data collected corresponds with research themes, and then report was produced.

4.10 Trustworthiness

Adler (2022) suggests that for research to be relevant it must be trustworthy. The four general criteria for trustworthiness are credibility, transferability, dependability, and confirmability (Stahl and King, 2014).

4.10.1 Credibility

Credibility determines if the research findings are a valid interpretation of the participants' original perspectives and represent plausible information derived from the participants' original data (Korstjens and Moser, 2018) . Studies reveal that the credibility of a study is determined when core-searchers or readers are confronted with the experience, they can recognise it (Nowell *et al*., 2017). To ensure credibility, the researcher conducted online interviews on Microsoft Teams; the interviews were recorded and transcribed with consent from the participants (see appendix 3). The researcher then listened to the recordings numerous times and made notes to ensure that the findings represent the true data from the participants.

4.10.2 Transferability

Munthe-Kaas *et al.* (2020), define transferability as an assessment of the degree to which the context of the review question and the context of studies contributing data to the review finding differ to a priori established characteristics (transfer factors). As suggested by Stahl and King (2014) that transfer of the results of this study is only possible when a thick description provides a rich enough portrayal of information system security vulnerability implications for application to South African financial firm's situations, and usually at the behest of the local constituents.

4.10.3 Dependability

Dependability involves participants' evaluation of the findings, interpretation and recommendations of the study such that all are supported by the data as received from participants of the study (Korstjens and Moser, 2018). In order to address the dependability issue more directly, Shenton (2004) suggests that the processes within the study should be reported in detail, thereby enabling a future researcher to repeat the work, if not necessarily to gain the same results. For this study, the interviews were conducted in order to address the research problem and the researcher retained all research documents, interview recording and all data to ensure that there is an audit trail for future.

4.10.4 Confirmability

Korstjens and Moser (2018) describe confirmability as the degree to which the findings of the research study could be confirmed by other researchers and is concerned with establishing that data and interpretations of the findings are not figments of the inquirer's imagination, but clearly derived from the data. Additionally, the role of triangulation in promoting such confirmability must again be emphasised, in this context to reduce the effect of investigator bias (Shenton, 2004). The researcher in this study had a coding method which specified the patterns found during the data analysis to ensure that when data was evaluated during data collection and analysis, conclusions were likely to be replicated by others. Further, to ensure that the study is not bias, the researcher interviewed participants from different financial institutions.

4.11 Ethical considerations

Fleming and Zegwaard (2018) suggest that at many educational institutions, to collect data from human participants for research purposes without ethical approval would place the researcher outside the institutions Staff Code of Conduct (often worded within the requirement of adherence to institutional regulations, which will include the Human Research Ethics regulation). The ethical clearance for the researcher was provided by the Humanities and Social Science Research Ethics Committee with Ethics Reference Number HS21/7/50 (see appendix 2). During the data collection the researcher informed the participants that their participation in the interviews is voluntary and may choose not to take part and may stop participating at any time they want to if they decide to participate. The researcher also informed participants that their personal details will be kept confidential, and that the data will be kept safe in the university premises and any online information will be protected with the relevant security processes and technologies (See appendix 4).

4.12 Chapter summary

In chapter four, the researcher focused on discussing the research design and methodology which was followed in this study. The in-depth view of research paradigm, research design research method, target population, instrument development, and sampling techniques was provided. The chapter outlined the pilot study, data Analysis, thematic data analysis, trustworthiness and ethical considerations of the study.

CHAPTER 5
FINDINGS AND RESULTS DISCUSSIONS

5.1 Introduction

This chapter outlines the main concepts and presents findings from the interview process conducted and associated data analysis. A brief description of the participants that were involved in data collection is provided and followed by the discussion on the key concepts linking to the research questions that were drawn from interviews. Lastly, it provides the concluding remarks.

5.2 Demographics

The researcher conducted a total of eight interviews with IT and cybersecurity professionals from different financial firms that were approached for data collection. The one-on-one semi structured interviews were conducted online using Microsoft Teams. The letter "P" was given to each participant, and the number next to the participant signifies the respondent's number, for example P1 = participant number one. The table below demonstrates participants of the study, gender, and job /roles of the participants.

Participant ID	Gender	Position
P1	Male	Chief Information Officer
P2	Male	IT Security Manager
P3	Male	Information Security Analyst
P4	Male	Head of Cybersecurity Engineer
P5	Male	Senior Information Security Officer
P6	Male	Information Security Analyst

P7	Male	Chief Information Security Officer
P8	Male	Information Security Analyst

Table 2: Participants, gender, and job/roles of the participants

The above table indicates that all eight interviews were conducted with male participants; these were the only participants from financial institutions that agreed to participate in the research. Studies show that the cybersecurity industry is male-dominated, which could be another reason the researcher could only get male participants. Research shows a reliable estimate of women in the cybersecurity workforce globally remains at 25% (ISC)2 Global Information Security Workforce Study, 2021). One of reasons why cybersecurity has not been able to achieve some level of gender equality is that there is still a preconception that technical professions are the best options for boys, not girls, among young girls and even their families (CyberWarrior, 2023). There is a need for organisations to diversify and hire more women in the cybersecurity field. Dallaway (2016) states that it was suggested that women bring a different mind-set and set of skills to the workplace, including attention to detail, analytical ability, and problem solving.

5.3 The level of cybercrime in South African financial sector

The aim of the research question in this section was to evaluate the level of cybercrime in the South African financial institutions. To address this research question, it was important for the researcher to understand the influence of technology changes on risks to firms, threats to the firms and what information system security and cybersecurity attacks do financial firms experience. The findings are discussed below.

5.3.1 Influence of technology advancements on risks to firms

The outcome from seven participants (P1, P3, P4, P5, P6, P7, P8) indicate that it is without a doubt that changes in technology have a lot of benefits to firms but can still cause disruptions in the security of systems. In contrast,

> *"I think bad actors will look for cybercrime no matter what the tech is, I do not think they are necessarily worried about the tech. If the tech is not built right, there will always be inherent risk, doing business alone is a risk."* [P2]

This means that security risks are always there, whether there is old or new technology and that adversaries can attack both legacy and new systems.

> *"The fast advancement of technology has brought numerous benefits to organisations, but at the same time it has created new pitfalls that must be managed."* [P8]

The main issue is that new risks emerge when technology evolves, adding to the current cyber risks problems.

> *"As soon as a new technology is developed or emerges, the threat actor or the hacker is busy finding a way to find weakness or vulnerability into that specific technology."* [P6]

> *"Because of that grey area of still having to adjust new ways of doing things into a current ecosystem; it brings a lot of other risks where knowledge/technology touch points are getting figured out. So, normally bad actors take advantage of such grey areas, they exploit while an organisation is still trying to find its foot/trying to understand. They normally know that there will have to be upgrades, overhauls, changes that must happen, so they usually normalise that gap."* [P1]

> *"The broad adoption of very varied technologies right from you know not only just that operating system at database level, but also in terms of data management platforms, storage platforms and then connect the connectedness and interconnectedness of systems. You obviously make the risk of security failures much higher, not just because of the rapid pace of change, but also because of that large technology footprint which brings with it inherent security weaknesses."* [P7]

In literature, Allison (2022) stated that as technology advances, so do hackers' abilities to identify weaknesses and flaws in organisations' security protocols; this creates a serious cybersecurity issue because the hackers are able to access the protected data and files. In conclusion, as technology advances, there is a gap for organisations to manage changes to meet business needs such as upgrading and configuring systems, training employees, and testing systems which increase risks in organisations. The Utica University (2023) also discussed that the frequency and sophistication of cybercrimes increase along with technological advancement, fortunately, as technology has developed, so too has the capacity to prevent cybercrimes from occurring and to defend people when they occur. The gaps mentioned above get exploited by the adversaries while organisations are still finding ways to manage the changes.

5.3.2 Threats to the financial firms

> *"Financial companies are a major target for cyberattacks because they hold a larger amount of sensitive data such as personal and financial information of customers."* [P8]

> *"The threat to financial institutions is more on the reputation and the perception of stability in the financial system."* [P2]

> *"Financial service is a data intensive industry, trust is paramount; any risk associated with a system compromise, right and loss of integrity of processing systems, any risk associated with data loss, and specifically customer data loss is a very high impact type risk."* [P7]

In literature it was discussed that financial institution's servers host data files that contain sensitive information, such as users' personal and financial information; this information is highly appreciated on the dark web (Subhani, 2023).

> *"Financial services risk appetite is very low and need to put all effort to ensure that they hunt and protect against bad actors; however, they are not the most targeted but probably easy frequently ones depending on who is sponsoring the attack and the reasons behind."* [P1]

The research findings revealed that another threat to financial firms is third-party vendors.

> "*I think the problem that people are experiencing at the moment is supply chain technology changes where they do not necessarily have an oversight of and visibility of what the third-party suppliers are doing in their environment which will have impact in your environment. I think the increase to risk as new technologies are introduced into third-party environments would be the biggest threat now."* [P4]

In literature, PwC (2023) argued that third party data breaches may force an organisation to respond to incidents that are outside of its control or originate from an indirect source; even though existing breach standards do not require the organisation to respond, the firm may nonetheless sustain serious reputational harm as a result of the occurrence.

> *"The biggest thing has been data breach and mainly their approach in terms of nonnecessary from the bank itself, but mostly from third party vendors that the financial services associate themselves with."* [P6]

The literature revealed that the attack against Nedbank occurred through the third-party service provider, which issues SMS and e-mail marketing information on behalf of the bank and several other companies (Moyo, 2020). Moreover, humans (employees and customers) in the financial sector have been identified as one of the threats.

> *"Customers get more attacks and that there have been instances where fraudsters try and sometimes successfully gain access to a customer's account via sim swap or even gaining accessing to the customer's mobile phone."* [P3]

> *"Another key one is the revenue and customer facing channels; a lot of financial sectors that will have online banking websites and mobile applications."* [P5]

As discussed in the literature, the country has seen a 100% increase in mobile banking application fraud and Mcanyana *et al*. (2020) state that it is estimated the country suffers 577 malware attacks an hour. Also,

> "*we would find the biggest kind of risks or areas of concern is our internal users and just a general user capability. You know what access the users have to specific items and at the end of the day you know people will always have access to certain things and we will be able to put things together in order to cross it and attacks or manipulate data cell data to certain syndicates, et cetera."* [P5]

Due to the access the employees have, it is easy to harm the security of the firm intentionally or unintentionally. Rosenthal (2021) in literature stated that a 47% increase in the number of incidents involving insider threats between 2018 and 2020 was reported; this encompasses intentional data exfiltration and data loss due to human error.

5.3.3 Security attacks in financial firms

Participants were unable to provide full details on the security attacks in the organisations due to the sensitive nature of the study. However, findings showed that organisations deal and investigate security events and incidents which occur on the network on daily basis; adversaries attempt to breach the firms daily.

> "*There are guys scanning the perimeter all the time trying to find holes and weaknesses that they can exploit. So, there's a lot of surveillance activity. There's a lot of phishing and there's a lot of malwares*." [P7]

For example,

> *"We get attacked daily. There are attacks that we know about and attacks we do not know about. Those we know are the ones that we would put protection for; we have things/tools to look for DoS, tools to look for people putting bad stuff in our websites and that goes for any service that we expose on the internet. Things we do not know about; we see a lot of impersonations on social media and setting up websites pretending to be the organisation in order to steal money from people. Unfortunately, we are not a tech savvy country, so people do not have much knowledge."* [P2]

These can be successful or unsuccessful attacks; participants mentioned that there have been no successful security incidents resulting to financial losses. Findings revealed three common attacks to the financial firms, namely, phishing, insider attacks and DDoS. The security attacks which firms experience on daily basis are presented below:

i. Phishing

Writer (2021) pointed out that in South African banks, the most common fraud of 2021 was phishing. For example,

> "*We have had a high number of phishing attacks in which attackers create fraudulent emails or communications that seem to be from reliable sources, such as banks, courier companies or other financial institutions."* [P8]

> *"We have a lot of attacks against those on the daily basis, lots of attacks via emails, there's a lot of unsuccessful events like commodities and phishing campaigns, but then some highly targeted phishing types of campaigns."* [P2]

In literature, Collard (2021) mentioned that in the coming year, attacks such as phishing emails, criminals might start applying artificial intelligence (AI) and emerging technology in their social engineering attacks, cloud jacking attacks and ransomware are expected to rise. Additionally,

> *"Work from home also played part, several machines were breached through phishing emails fortunately we were able to quickly respond to that on time. Still unclear if internal or external. There was also a phishing email received because of a breach of a third-party."* [P1]

The three distinct ways of phishing during the pandemic as discussed by Walker (2020) in literature were;

a) Phishing attacks providing basic information about the pandemic, and spam/scam emails advertising dubious goods and services, were part of the first wave.
b) The second wave introduced fresh, and novel phishes, with cybercriminals attempting new strategies to convince users to view malicious content.
c) The researchers have seen repurposed standard phishing models converted into corona-virus-related phishing scams in the third wave.

ii. Insider attacks

"*Weakest link in the value chain of technology is human, internal people, because security works from a zero-trust perspective so there are also people that need to be filtered; multiple things including their knowledge, personal interests, aspirations, experience, etc. For example, If we have a disgruntled employee, that becomes a big risk as they might expose sensitive information. Employees are the weakest link, sometimes they do not do it intentionally by clicking malicious links*." [P1]

Ohanian (2021) stated that it is predicted that insider data breaches will rise 8% in 2021 and that a third of all incidents will be caused internally.

"There was an entry at their firm which was gained through an employee and data was stolen in their firm, however there was no password hit." [P3]

Another example pointed out,

"*We have had insider threats whereby staff members or outside contractors who have access to sensitive data mistakenly or maliciously breached our data by leaving reusing passwords and linking company emails with their social media accounts*." [P8] iii. Distributed Denial of Services (DDoS)

"*Sometimes we deal with DDoS attack, in which attackers flood our public online platforms mainly to make them unavailable to users so that they destruct us and attack other things while we deal with that. That obviously causes significant financial losses and damage to our reputation as the company*." [P8]

The participants interviewed revealed that in their companies there have not been direct financial losses due to the security attacks experienced. However,

> *"I think small reputational damage but obviously the reputation of damage translates into financial loss if you think about it. Let's say there's a reputational damage for certain financial service and details or information is out there in the wild. What is your next step? Your next step is leaving those banks. I'm going to another bank where my data will be more secured. So that's the bank losing a client and you losing a client. There's financial loss."* [P6]

As discussed in literature, cybersecurity breaches can lead to a loss of trust in the company and negative publicity that could damage its brand and reputation (Dosal, 2023).

5.3.4 Addressing security attacks

To assess the state of readiness of financial institutions to address cybercrimes the researcher asked participants ways in which the cybersecurity attacks are addressed within the organisation. The respondents mentioned ways in the figure below as ways in which security attacks are usually addressed and how they prepare for the future attacks.

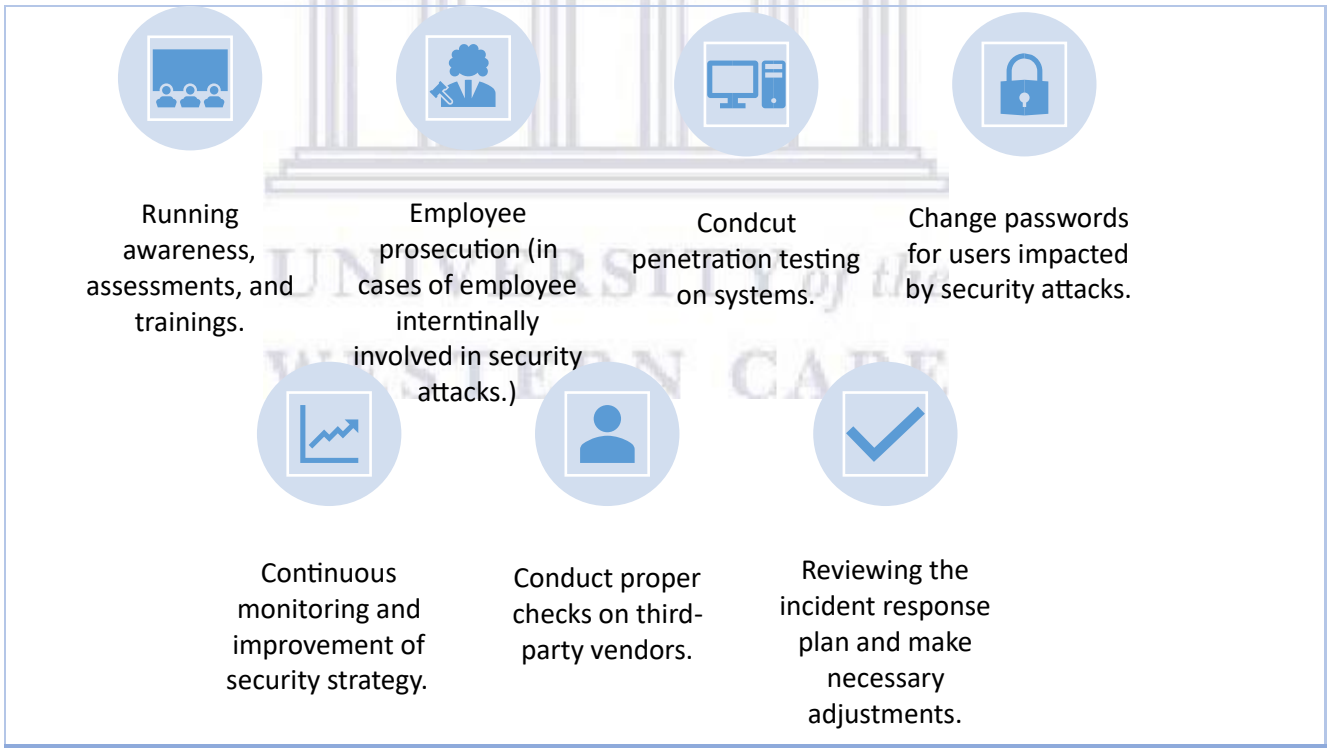


Figure 8: ways in which security attacks are usually addressed (Source: Researcher, 2023)

5.4 The level of South African financial firms' investments towards the information systems security

It was significant for the researcher to understand whether the South African financial firms invest in information system security or cybersecurity. To address the research question, the researcher formed themes. These themes were set to discover the understanding of cybersecurity/information system security, what strategies do firms implement for security and the challenges they encounter during the process.

5.4.1 What is Cybersecurity/information systems security

The findings from all eight participants showed that participants are familiar and understand what information system security or cybersecurity is. The participants described the terms as follows:

> "*The primary method you need to apply is ensuring that there is layered security across your environment and not thinking that a single solution will provide security in your environment. I think that is one of the foundational pillars on ensuring security is making sure that you have the respective layers in place; so whether or not you got Identity and Access Management, you got the ability to have your firewalls in place on the parameter, making sure that you have data leakage prevention in place, you got vulnerability management in place, that you got all of these layers that challenge and make your environment harder to infiltrate or exfiltrate data or manage and ensure that your security practices are constantly looking at hardening elements and areas of your business without putting your security in one particular technology or layer to prove your stance in your cybersecurity space."* [P4]

> *"I would define information systems security the ability to understand all technologies within your company and how they are used to specifically protect against external and internal threats by both a technical configuration perspective as well as just general user awareness, and the socialisation of security within the environment."* [P5]

> Additionally, "*It is the protection of electronic systems, networks, and data from unauthorized access, use, disclosure, tampering, modification, or destruction. The goal of cybersecurity is to ensure the privacy, integrity and availability of information and resources in the appearance of various cyber threats such as malware, phishing, ransomware, and other forms of cyberattacks ."* [P8]

The literature supports the definitions provided by participants, for example, the International Telecommunication Union [ITU] (2018;2019;2020) defined cybersecurity as the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the cyber environment and organisation and user's assets. Similarly, the Tip (2019) in literature defined cybersecurity as the process of protecting networks, devices, and data from unauthorised access or illegal use and maintaining the confidentiality, integrity, and accessibility of information. Participants provided other descriptions of cybersecurity, such as:

> *"I think it is very much like information security, it perhaps focuses more on internet type of threats, but it is essentially looking after all your assets and making sure that you protect them."* [P2]

> "*Cybersecurity is the protection of IS and protects the unlawful usage of the systems."* [P3]

> *"So, you know, in my context, cybersecurity and information security blend together cyber. You know, there are many definitions, but in my world you know, I think cybersecurity supersedes information security, purely because there is very little done, there is no longer digital right. So, if I were to define information security in the digital age, I'd call it cybersecurity."* [P7]

> *"So, information security focuses more on data confidentiality, integrity, and availability, that's how I see it. And when you speak of cyber, it's not looking at digital assets."* [P6]

5.4.2 Cybersecurity strategies in financial institutions

Findings revealed that the organisations need to implement effective strategies that with security tools that protect the specific systems and data of the firms.

> *"So, you need a strategy that allows you to protect your systems. So that's a, you know, that's a given and it's what we want."* [P7]

> *"So, from a strategy perspective, you will need to have an effective security program. And what I mean by that from a secure effective security program is having the right tools. So, tools which actually bridge that gap of where threats or the risks are you need the right skills."* [P6]

The strategies indicated by participants during the data collection are discussed below.

i. Knowing your assets

> "*The biggest saying is that you cannot protect what you do not know. So, the first thing is to make sure that we know what we have.*" [P2]

In literature, the Qualys, Inc (2023) argued that attackers target external assets and software that are not visible to security practitioners that rely on conventional attack surface management and vulnerability management solutions alone; to reduce cyber risk and bridge the IT security gap, the modern enterprise must be able to achieve complete visibility of both internal and external internet-facing assets.

ii. Cybersecurity frameworks and industry best practices

> "*One of the main things is a security framework and its generally composed of within different companies of different frameworks and standards. Companies in those strategies essentially create what is called an isms information security management system (ISMS) program whereby we collect a variety of different frameworks and standards and tailor for our specific company which include best practice frameworks and standards such as COBIT, NIST, CIS, ISO 27001 which are used in order to formulate the program with regards to covering governance, technical security controls, human controls, data security, privacy, human resource security, physical security. So, we cover it from many different angles, but the strategy is essentially both of best practice frameworks and industry-based practices as well as strategic objectives of the company*" [P5]

The literature discussed that cybersecurity standards determine the requirements that an organisation should follow to achieve cybersecurity objectives and facilitate against cybercrimes and demonstrate whether an information system can meet security requirements through a range of best practices and procedures (Taherdoost, 2022), and the participant who responded shared a similar viewpoint with this.

iii. Protection at seven layers of technology

As described in literature, layered defense is the concept of securing a computer network using a number of defensive tools such that, in the event that one fails, additional tools are already in place to block an attack (Chellappan *et al*., 2015).

> "*In our environment, without going into details about it, we obviously look into all the seven layers of technology. Looking at each layer; the user layer of interface, where there are applications and systems, that layer, because it is a touch point in a form of a laptop that has an application layer on top of it, the rules that play in it because of the way people access the layer are different. Our strategy ensures that each layer according to the OSI layer has its own demands as there are different protocols that run at each layer. Each layer has its own strategy, it has its own requirement. You put the defense mechanisms based on the protocol that run and the sensitivity of each layer. For example, we can't have too many people accessing the data layer from external; it is accessed internally. What you put on top in the defense strategy, they all have to sort of align*." [P1]

GoJ (2015) in literature supports the participant's view, stating that it is necessary to ensure multi-layered cybersecurity for the realization of a society in which citizens can live safely and securely, through the cooperation of multi-stakeholders, including government bodies, local governments, cyber-related businesses, critical infrastructure operators, educational and research institutions, and every individual iv. Identity and Access Management

IAM system in literature, was defined as a framework for business processes that facilitates the management of electronic identities and includes the technology needed to support identity management (Dhamdhere, Karande and Phatak, 2017).

> *"We create clear roles and responsibilities for system access and use authentication and authorization mechanisms such as passwords and two-factor authentication to help ensure that only authorized users can access the systems."* [P8]

In literature, Dhamdhere, Karande, and Phatak (2017) suggested that IAM technology can be used to initiate, capture, record and manage user identities and their related access permissions in an automated fashion; this ensures that access privileges are granted according to one interpretation of policy and all individuals and services are properly authenticated, authorised, and audited.

v. Data protection

As suggested by Crocetti (2021) in literature, there is limited tolerance for downtime that can prevent access to crucial information, as a result, a key component of a data security strategy is making sure that data can be swiftly restored after any loss or damage. To ensure data is

protection,

"*We encrypt sensitive data at rest and in transit and implement data loss prevention strategies to help protect from data theft and unauthorized access. Implement firewalls, intrusion detection and prevention systems including VPNs to secure the organisations networks and prevent unauthorised access."* [P8] vi. Detection systems

"The second component is the ability to detect system compromises and detect security breaches because you're not always going to be able to prevent them, right?

So, there are challenges associated with being able to with such things, such a thing as 100% security. So, you do need to at some point also invest in detection capabilities. That's the second component." [P7]

In literature, it was discussed that an Intrusion Detection System (IDS), a) monitors and assesses normal network or computer system activity to find security risks or threats like denial-of-service (DoS), b) performs the process of recognizing malicious cyber-attack behaviour, and c) helps to discover, determine and identify unauthorised system behaviour such as unauthorised access, or modification and destruction (Sarker *et al*., 2020).

vii. Containment capabilities/Incident response readiness

"So, if you think about it in terms of the evolution of the cybersecurity breach, what you want is the ability to prevent a breach in the first place. But you can't always guarantee that. So, then you want to know where that it's happening. So, you want to detect it and then if you do detect it, you want to minimize impact. And in order to do that, you need a structured strategy for containment of a security breach so that it doesn't spread." [P7]

***"**And also have an effect of focus on Incident response readiness. You know, if there's an incident emerges, you need to be ready. You can't just do things on the fly. So, you need to have a proper incident response reading, incident response team, and that team needs to practice incident responsiveness should an incident ever occur."* [P6]

To support the participant's views, Fox (2020) in literature suggested that in the case of a security breach, an incident response plan ensures that the appropriate individuals and procedures are in place to successfully deal with the attack and allows companies to perform

a structured investigation to give a focused response to contain and remediate the threat. viii. Cybersecurity trainings

> *"We do regular training on cybersecurity best practices and simulated phishing exercises which help employees to identify and avoid potential threats."* [P8]

Koigi (2020) in the literature revealed that cyber threat actors' increased attention on South Africa due to linked factors such as lack of cybersecurity investment, the growth of cybercrime laws and law enforcement training, and limited public awareness of cyber threats. P3 mentioned that the strategies in their firm include mostly compliance videos (user awareness videos, they explain attacks, cybersecurity on system and ways to prevent) and messages displays on banking profiles for customers.

5.4.3 Challenges faced when implementing strategies of information systems security

Financial firms, just like other businesses, select and implement best strategies to ensure security and protection against internal and external threats. Even so, there are still challenges faced in the process. During the interviews participants revealed various challenges usually encountered when implementing cybersecurity strategies, see figure and discussion below:

i. Business buy-in

The first challenge to financial firms is business buy-in. The successful and use of a security strategy implementation must be stakeholder and business buying-in to the idea. For example,

> *"One big challenge is engaging with business units to convince them or to provide a security service that will assist with their enablement as opposed to being viewed as a blocker and we found very much that business units that engage with us first prior to undertaking a new project or implementing a new technology find that the implementation path is a lot smoother and more conducive to a better outcome than when they come to us at the end of a tech discussion or implementation."* [P1]

> *"The most difficult things to achieve is to get people who are not security experts to understand what the importance and the value of security is."* [P5]

In literature it was discussed that despite the fact that boardroom discussion of cybersecurity is increasing, many CISOs still struggle to gain executive support and understanding since various board members frequently have varying opinions on what cybersecurity is and how it

relates to privacy, data protection, and regulatory risk and others focus on risk postures, but few have an in-depth grasp of cybersecurity (Daswani and Elbayadi, 2021).

ii. Availability

Secondly, as financial firms provide online services to customers, it is important to ensure that there are no outages. The literature mentioned that as far as we are aware, the fundamental goal of Denial of Service (DoS) attacks is to make an information resource unavailable, or, to put it another way, to reduce information availability (Qadir and Quadri, 2016). Too much traffic and successful attacks to the business can affect the availability of the services; this is worrisome to companies.

> "*If you look at your banks and I guess our organisation as well, the biggest focus is essentially on availability of online services. So, if one causes any form of outage, it's a huge hit to business*." [P6]

For example, "*A bank experiencing systems failure meant 600,000 customer payments and direct debits went missing. The failure was caused by the bank's IT infrastructure struggling to deal with traffic volumes."*, PwC (2023).

iii. Budget, lack of skills, and lack of resources

The third challenge to financial firms is not having enough budget for cybersecurity.

> "*It is important that firms prioritise and understand the environment. Prioritising and understanding the company's environment ensures that firms know exactly what to secure, when to secure and what firms have the capability to secure."* [P5]

The literature revealed that the most recent Mimecast State of Email Security 2022 report, which analyses responses from 1400 IT and cybersecurity professionals across 12 different countries, South African organisations devote on average only 12% of their IT budgets to cyber resilience, which is less than the global average of 14% (ITWeb Security Summit, 2023). Moreover, the findings show that the lack of budget has contributed mostly to lack of resources and skills in South African organisations.

> "*Sometimes, implementing successful information system security methods involves significant financial, human, and technological resources; many businesses might not have the resources to make adequate investments in these areas*." [P8]

"I think skills is a massive problem, especially in cybersecurity workplace. I think that technology is maturing but I do not know if we have the right technology for it; I think as we do more, we figure out that we do not know much." [P2]

"When procuring certain systems and things and controls that we'd like to have in place, there's always cost money and unfortunately there's not a single financial services company that is perfect and has unlimited budget for security. Umm, so that's also something that we have to consider. The challenge we face is that we have to manage our security posture and program in an efficient way that we make use of the best possible. Tooling and the resourcing that we have is based on the budget that we are given." [P5]

The literature revealed that Jager, *et al*., (2023) states that there are several challenges, such as lack of time, lack of funding and lack of resources, that South Africa must overcome in order to address the cybersecurity skills gap. iv. Regulatory compliance

Findings show that regulatory compliance is another issue that is faced when implementing cybersecurity strategies in organisations.

"*Companies could be required to abide by a variety of laws and guidelines pertaining to information security, including the General Data Protection Regulation (GDPR) and the Payment Card Industry Data Security Standard (PCI DSS). These regulations might be difficult to follow and take a lot of effort."* [P8]

Terry (2022) in the literature stated that regulators require that financial institutions adhere to a wide range of cybersecurity compliance standards; regrettably, there are divergent expectations across regulators, which makes it more challenging for financial institutions to set clear goals.

v. Effective use of detection technologies and building playbooks

Lastly, findings revealed that other challenges are around the effective use of detection technologies and building playbooks.

"While technologies like a security information and management SIEM are mature, the companies deploying them usually are not always in step with that level of maturity." [P7]

This means that the technology can do it, but your ability to define events that need to be alerted to inside the same technologies are not always that obvious. As a result of the issue above,

> "*there is a big challenge around building playbooks and building and detection scripts that you know that are relevant to your business and to your technology landscape and so on. So, there's quite a big challenge around effective deployment of detection, use technologies and then containment is probably the hardest because.*" [P7]

Financial firms need to ensure that these challenges are taken into consideration during the implementation of the strategies.

5.5 Chapter summary

The chapter presented main concepts and presents findings from the interview process conducted and associated data analysis. The data was collected from 8 participants. This chapter provided a description of the participants that were involved in data collection and followed by the discussion on the key concepts linking to the research questions that were drawn from interviews. In the discussion of the concepts, the findings were supported by the literature outlined in chapter 2.

CHAPTER 6

CONCLUSIONS, RECOMMENDATIONS, AND IMPLICATIONS OF THE STUDY

6.1 Introduction

This chapter presents the conclusions, recommendations, and the implications of the research. It presents the conclusions made from the literature and primary study to address the research questions. It further outlines the recommendations from the study, limitations of the study, suggestions for future research and the summary of the thesis.

6.2 Conclusions from literature review

Chapter 2 presented the literature of this study. The discussion from previous research reports revealed that there has been significant growth in cyberattacks over the years. Lazic (2021) mentioned that cybercrime is perpetrated 2,244 times each day on average; every half a minute, hackers attack people worldwide. Goodman *et al*. (2015) revealed that the advanced infrastructure in South Africa is being used as a base for regional cybercrime activities. Due to the nature of the industry, financial institutions are among the six most targeted industries for cyberattacks (Manship, 2022). Some studies in this research revealed that there has been a significant increase in the rate of cybersecurity attacks ever since the world was hit by the COVID-19 pandemic, including SA. Pinnock (2020) believes that the COVID-19 pandemic escalated the rate of attacks. Mimecast Threat Intel (2020) also found a75 % rise in impersonation fraud in South Africa. The types of cybercrimes which pose the greatest information systems security risks were discussed, these are; the internet of thing (IoT) attacks, cloud attacks insider attacks blockchain and cryptocurrency attacks, machine learning (ML) and artificial intelligence (AI) attacks, hacking, email bombing and spamming, phishing, vishing, distributed denial-of-service (DDoS) attack, identity theft, ransomware, software piracy, salami slicing attack, trojans, card fraud, web jacking, smishing, and ATM malware.

This study revealed that financial firms in South African and all other industries including other countries are negatively impacted by the cybersecurity attacks. The impacts of cybercrime were highlighted to be financial losses, reputational damage, operational disruption, legal and regulatory consequences, intellectual property theft, and customer trust and loyalty (Sprintzeal Americas Inc., 2023). It was also a recommendation from it to put in place strategies to defend against the attacks. This will prevent cyber terrorism, cyber warfare, and cyber espionage threats (Seemma, Nandhini, and Sowmiya, 2018). The past studies discussed security risk assessments, cybersecurity policies, incident response policy, network security policy, password policy, physical security policy, national cybersecurity policy framework, and cybersecurity insurance as processes and policies to consider in implementing the effective cybersecurity strategy. Additionally, the suggested cybersecurity standards and frameworks for financial firms are the NIST, ISO 27001, COBIT, ITIL, PCI DSS, and CIS controls.

South African firms have implemented the cybersecurity strategies, however, Pygma Consulting (2021) suggested that South Africa, like the rest of Africa, is falling behind in terms of cybersecurity, and its government is grappling with issues such as a lack of ICT skills and coordination between inter-governmental departments. South African organisations with the

assistance of its government have to ensure that these issues are addressed. The studies in the literature discussed the lack of preparedness and cybersecurity challenges as factors that contribute to information systems security vulnerabilities in South African financial institutions.

6.3 Conclusions from the main study

The data of this study was collected from seven financial firms. The researcher conducted semi-structured interviews through an online platform, Microsoft Teams, and those interviews were recorded. All participants of the study were IT and Cybersecurity professionals and were males; this could have resulted due to the lack of diversity and skills in the cybersecurity industry. Organisations still need to hire more women in the field. To address the main and sub-questions research questions, the researcher developed nine open-ended questions to ask participants during the interviews.

6.3.1 Conclusions for objective 1: To understand the level of cybercrimes in the South African financial sector.

While the findings indicated that there are always cybersecurity risks whether there are legacy or new systems; the adoption of new technologies was pointed out to be one factor that contributes to new emerging threats. Participants revealed different threats to financial firms, and all applied to the firms as they are in one industry and have similar experiences. The threats identified include adversaries wanting to steal sensitive data, breach third-party vendors, and exploit employee and customer vulnerabilities. Moreover, the outcome of the study indicated phishing, DDoS, and insider attacks as the most common security attacks in the financial firms.

6.3.2 Conclusions for objective 3: To evaluate the state of readiness of financial institutions to address cybercrimes.

To ensure that firms address the cybersecurity attacks, participants indicated that they run awareness, assessments, and trainings. Secondly, organisations in cases where they are intentionally involved in a breach Prosecute an employee. It is recommended that firms conduct penetration testing to identify any weaknesses in their systems and find security controls for the identified vulnerabilities. Furthermore, firms are advised to enforce password change and continuously monitor and improve cybersecurity strategies. Lastly, it is suggested in this study that conducting proper checks (relating to cybersecurity) on thirdparty vendors and reviewing the incident response plan and make necessary adjustments is key.

6.3.3 Conclusions for objective 2: To examine the level of South African financial firms' investments towards the information systems security.

All participants showed an understanding to information system security. Participants indicated different cybersecurity strategies they implement, these include; knowing your assets, cybersecurity frameworks and industry best practices, protection at seven layers, Identity and Access Management, Data protection, Detection systems, Containment and Incident Response, and cybersecurity trainings.

6.3.4 Conclusions for objective 4: To identify challenges that are encountered by South African financial institutions when implementing cybersecurity strategies.

While the firms implement the strategies mentioned above, participants revealed that they experience challenges such as business buy-in, availability of services, budget, skills, resources, regulatory compliance, building playbooks, and effective use of technologies.

In consideration of the responses, the threats and challenges discussed have been noted as the factors that contribute to information systems security vulnerabilities in South African financial institutions.

6.4 Recommendations

As cybercrime continues to be an on-going issue in the world, there are recommendations what companies can do in order to prevent against the attacks. The participants and literature suggest the strategies below to use in the firms to improve information system security to reduce risks in the organisations.

Developing a cybersecurity strategy

The first recommendation is that organisations should ensure that they develop a cybersecurity strategy that will allow them to have appropriate tools or systems to not only detect threats but also prevent them. According to Check Point Software Technologies Ltd

(1994-2023) corporate cybersecurity strategy should be tailored to an organisation's unique security needs as small, medium, and large businesses in different industries and locations can face very different threats and have different security requirements. For example, one participant mentioned that for companies to reduce information system security risks, they must have an effective security strategy that: a) works for the team or company, and b) aligns with the business strategy, not purely for security because if the business and security are

working in silo, buy-in might never be obtained. The participant added that to have an effective security program means having the right tools that will bridge that gap of where the risks are you need the people with the right skills to do the work.

Conduct cybersecurity risk assessments

A participant shared that a lot of firms may not understand what their core components are that they need to protect, and they may go about implementing controls that they have read about or been told to implement but that is not necessarily addressing the core risk to their environment. To have effective cybersecurity, the study revealed that companies must continuously perform risk assessments to be able to understand protecting and identifying gaps to improve the security of the company. IT Governance Ltd (2023) mentions that a cybersecurity risk assessment helps to ensure that the cybersecurity controls that a company choose are appropriate to the risks the organisation faces. One participant mentioned that if a company knows how secure or how insecure they are, then they can effectively address cybersecurity issues relating to them. Performing risk assessments will help firms put the right controls in place to ensure that the assets of the firm are secure.

Complying with cybersecurity standards and frameworks

The findings of the study revealed that firms must comply with the industry cybersecurity standards and adopt frameworks to guide them with the steps organisation must take to evaluate, manage, and reduce cybersecurity risk. Further, one respondent mentioned that one of the main things is a security framework which is generally composed of within companies of different frameworks and standards. Respondents suggest that the financial firms should use the security controls as advised in the security frameworks and standards to best fit the firm's strategy.

Ensure security in all layers

The study recommends that organisations implement a layered security approach. In literature it was discussed that layered defense is the concept of securing a computer network using a number of defensive tools such that, in the event that one fails, additional tools are already in place to block an attack (Chellappan *et al.,* 2015). A participant mentioned that it is prudent to have a multi-layered security to discourage attackers. For example, the participant stated that each layer has its own strategy and requirement, and the defense mechanisms are placed based on the protocol that run and the sensitivity of each layer.

Implement a multi-factor authentication and Strong password policy

A participant recommended that firms should implement a multi-factor authentication policy for when users access systems or data in the business to add an extra layer of security. MFA reduces the risk of password cracking, phishing, or credential stuffing, as it makes it harder for attackers to access your accounts (Identity and Access Management, (2023). Additionally, it is suggested that firms establish a strong password policy, where employees use difficult and unique passwords and companies should also forbid the reuse of previous passwords and require frequent password changes.

Update systems and software

As stated in literature by Patel (2021), if an app was not designed with cloud connectivity in mind, it is likely to be exposed to today's cyber threats, as a result, more contemporary encryption standards may not be compatible with certain older assets. Additionally, Ancell (2021) mentioned that businesses that use outdated legacy technology increase their cybersecurity vulnerabilities. With the issues stated above, a participant recommended that firms keep systems and software up to date on a regular basis. Updating systems and software ensures that vulnerabilities are patched and the risk of being exploited by adversaries reduces.

Network segmentation

A participant recommended that firms implement network segmentation to improve security. An example provided by Cisco Systems, Inc. (2023) of implementing segmentation in a large bank with several branch offices is "*The bank's security policy restricts branch employees from accessing its financial reporting system. Network segmentation can enforce the security policy by preventing all branch traffic from reaching the financial system. And by reducing overall network traffic, the financial system will work better for the financial analysts who use it.".* Additionally, Network segmentation provides unique security services per network segment, delivering more control over network traffic, optimizing network performance, and improving security posture (VMware, Inc., 2023).

Cybersecurity awareness

The study revealed one of cybersecurity issues in South Africa as the lack of awareness among users (employees and customers) and organisations the study advises that companies should raise awareness to employees and customers. A participant suggested that the financial firms should regularly teach employees on cybersecurity best practices. Mimecast Services Limited

(2003-2023) suggests that an effective awareness training program addresses the cybersecurity mistakes that employees may make when using email, the web and in the physical world such as tailgating or improper document disposal. For example, to train employees, one of the participants revealed that the company provide hands on exercises to employees on how to spot phishing emails and how to report security problems.

6.5 Limitations of the study

While every attempt was made to complete the study as planned, this study had some potential obstacles that were not resolved. Given the nature of cybersecurity and the sensitive nature of the information associated with cybersecurity, there was resistance in obtaining detailed reports from previous security breaches experienced by the institutions. Additionally, the information provided by the institution was carefully camouflaged in order to prevent the leak of critical information. With the sample group being only the employees of these financial organisations, there was limited access to those participants as well as the not gaining a complete view of the factors that influenced previous security breaches that the institution experienced. The data could also be skewed in a light that will serve to minimise the impact of the breaches the institution might have encountered.

6.6 Suggestions for future research

The current study is conducted with is limited number of financial firms; it might not represent the views and experiences of all financial institutions in Cape Town. It would be good that the future research would be conducted with a larger sample as well as be extended to financial institutions in other provinces of the country. These results would reflect overall views and experiences of all financial institutions in the country.

Additionally, it would be helpful to include financial institutions customers as participants to the study. This would provide insights on how cybersecurity targeted at customers affect both financial institutions and customers and help the firms in improving the security of customer facing systems. Additionally, customers as participants would bring more insight on the nature attacks targeted to them; this would help companies understand their customers and find ways to increase user awareness.

Moreover, the study presents potential for future research to be conducted to assess the effectiveness of current cybersecurity strategies and policies. This would help in exploring and identifying which strategies and policies that are the best under certain use cases and identify

areas for improvement if it needs to be. Having strategies and policies best suitable for the different use cases as they occur will help organisations stay cyber resilient.

Further, as cybersecurity has become a problem affecting not only companies but citizens as well, it would be interesting to investigate on how government and companies work together to raise awareness and combat cybercrime. Well informed and vigilant citizens would help reduce cybersecurity issues for the South African economy.

6.7 Conclusion of study

This study commenced in 2021 with the creation and defense of a research proposal. The study sought to evaluate the implications of the information system security vulnerabilities in Cape Town financial institutions.

Chapter 1 outlined the objective of the study which was to understand the factors that contribute to information systems security vulnerabilities and their Implications for South African financial firms in Cape Town. Additionally, chapter 2 discussed the available literature related to the research aims and the primary and secondary questions of this study.

The information security standards that guide organisations were then discussed in chapter 3 and chapter outlined the research methodology and design for the study. Findings from the data collection were presented and discussed in chapter 5.

It is without a doubt that adversaries exploit the vulnerabilities in organisations to gain access; weaknesses can be in employees and systems of a company. The study found that even though firms South African firms implement cybersecurity strategies, there is still factors such as adopting the use of technology, lack of awareness of employees and customers, lack of resources, skills and budget, third-party vendor security posture, effective use of systems, and regulatory compliance that still need to be addressed. It is recommended that organisations have effective an effective strategy, perform risk assessments, complying with cybersecurity standards and frameworks, have layered security, raise awareness, implement network Segmentation, update systems and software, implement a multi-factor authentication as well as strong password policy. South African organisations still have a lot of gaps to address. Further, the study provided suggestions for future research.

7. REFERENCES

Abomhara, M., Køien, G. M., and Alghamdi, M. (2015). Cyber security and the internet of things: Vulnerabilities, threats, intruders and attacks. *Journal of Cyber Security and Mobility*, *4*(1), 65–88. https://doi.org/10.13052/jcsm2245-1439.414

Accenture Security. (2019). The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study. *Ninth Annual Cost of Cybercrime Study*, 18. Available at: https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019Cost-ofCybercrime-Study-Final.pdf#zoom=50 (Accessed 2021). Adedoyin, O.B. (2020). Quantitative Research Method. Available at:
https://www.researchgate.net/publication/340594200_Research_Methodology (Accessed: 29 July 2023).

Adler R.H. (2022). Trustworthiness in Qualitative Research.
Journal of Human Lactation, volume 38, no 4, pp. 598-602. https://doi.org/10.1177/08903344221116620

Adu, K. O., and Badaru, K. A. (2022). What Makes the Significance of the Study Plausible?. Available at: https://www.researchgate.net/publication/358089835_What_Makes_the_Significance_of_the_Study_Plausible (Accessed: 5 August 2023).

Africa, S. (2020). In South Africa , Cybersecurity investments are needed to mitigate increasing risks amid COVID-19 pandemic. Available at: https://fticybersecurity.com/wp-content/uploads/2020/05/Covid-19Cybersecurity-Risk_South-Africa_FTI-Consulting.pdf (Accessed: 22 October 2021).

Aggarwal, G. (2021). How The Pandemic Has Accelerated Cloud Adoption. Available at: https://www.forbes.com/sites/forbestechcouncil/2021/01/15/how-the-pandemic-has-acceleratedcloudadoption/?sh=728522486621 (Accessed: 24 October 2021).

Al Mehdar, Z. (2020). Cybersecurity and Cloud Computing: Risks and Benefits. Available at: https://rewind.com/blog/cybersecurity-and-cloud-computing-risks-and-benefits/ (Accessed: 24 October 2021).

Alawida, M., Omolara, A.E., Abiodun O.I., and Al-Rajab M. (2022). A deeper look into cybersecurity issues in the wake of Covid-19: A survey, J King Saud Univ Comput Inf Sci. 2022 Nov;34(10):8176-8206. doi: 10.1016/j.jksuci.2022.08.003. Epub 2022 Aug 11. PMID: 37521180; PMCID: PMC9367180.

Alfreds, D. (2016). ATMs 'vulnerable' to cyber hacking. Available at: https://www.news24.com/fin24/archive/tech/cyber-security/atms-vulnerable-to-cyber-hacking-20160503 (Accessed: 17 October 2021).

Algosec. (2023). The network security policy management lifecycle: How a lifecycle approach improves business agility, reduces risks, and lowers costs. Available at: https://www.algosec.com/wpcontent/uploads/2017/08/algosec_network_security_policy_management_lifecycle_wp.pdf (Accessed: 6 August 2023).

Allen, K. (2021). South Africa : South Africa lays down the law on cybercrime [WWW Document]. Institute for Security Studies. Available at: https://issafrica.org/iss-today/south-africa-lays-down-thelaw-oncybercrime (Accessed: 12 October 2021).

Ahatlan, K. (2022). 7 Ways IoT device security can fail. Available at: https://www.intertrust.com/blog/7-waysiotdevice-security-can-fail/ (Accessed: 9 August 2023).

Akhtar, I. (2016). Research Design. Available at: https://www.researchgate.net/publication/308915548_Research_Design (Accessed: 25 April 2021).

Almalki, S. (2016). Integrating Quantitative and Qualitative Data in Mixed Methods Research—Challenges and Benefits. Journal of Education and Learning, 5(3), 288. https://doi.org/10.5539/jel.v5n3p288

Amos, Z. (2022). Hidden Benefits of Diversity in Cybersecurity. Available at: https://informationsecuritybuzz.com/hidden-benefits-of-diversity-in-cybersecurity/ (Accessed: 15 April 2023).

Ancell, B. (2021). Top 5 Risks of Using Outdated Technology. Available at: https://www.whymeridian.com/blog/top-5-risks-of-using-outdated-technology (Accessed: 29 October 2021) Anoruo, C. (2019). Employing COBIT 2019 for Enterprise Governance Strategy. Available at: https://www.isaca.org/resources/news-and-trends/industry-news/2019/employing-cobit-2019-forenterprisegovernance-strategy (Accessed: 13 June 2022).

Anderson, J.L. (2023). Global cyberattacks increased 38% in 2022. Available at: https://www.securitymagazine.com/articles/98810-global-cyberattacks-increased-38-in-2022 (Accessed: 29 July 2023).

Ansari, M.R., Rahim, K., Bhoje, R., and Bhosale, S. (2022). A STUDY ON RESEARCH DESIGN AND ITS TYPES. International Research Journal of Engineering and Technology (IRJET), Volume: 09, Issue: 07, pp. 1132-1135.

Ascend IT Solutions, Inc. (2021). The Impact of Ransomware. Available at:https://www.ascenditsolutions.com/blog/executive-summary/65-the-impact-of-ransomware#:~:text=The%20impacts%20of%20a%20ransomware,generating%20operations%20being%20shut%20down (Accessed: 22 October 2021)

Ashley, M. (2021). Top 10 Common Software Vulnerabilities. Available at: https://devops.com/top-10-common-software-vulnerabilities/ (Accessed: 29 October 2021).

Asiamah, N., Mensah, H. K., and Oteng-Abayie, E. F. (2017). General, target, and accessible population: Demystifying the concepts for effective sampling. Qualitative Report, 22(6), 1607–1621. https://doi.org/10.46743/2160-3715/2017.2674

Atmowardoyo, H. (2018). Research Methods in TEFL Studies: Descriptive Research, Case Study, Error Analysis, and R and D.Journal of Language Teaching and Research, Vol. 9, No. 1, pp. 197-204. DOI: http://dx.doi.org/10.17507/jltr.0901.25

AXELOS Limited. (2019). ITIL Guiding Principles for Continual Improvement. Available at: https://www.axelos.com/resource-hub/white-paper/itil-guiding-principles-for-continual-improvement (Accessed: 8 June 2022).

Babbie, E. (2010) The practice of social research. 12th Edition, Wadsworth, Belmont.

Baker and McKenzie. (2021).

Africa: Implementation of cybersecurity and data protection law urgent across continent. Available at: https://insightplus.bakermckenzie.com/bm/data-technology/africa-implementation-of cybersecurity-and-dataprotection-law-urgent-across-continent (Accessed: 30 October 2021).

Balbix, Inc. (2023). Using Artificial Intelligence in Cybersecurity. Available at: https://www.balbix.com/insights/artificial-intelligence-in-cybersecurity/

Barlow, E. (2023). What makes SA a target for cyber crime, what actions can be taken?. Available at: https://www.itweb.co.za/content/Pero37Z34ydMQb6m (Accessed: 29 July 2023).

Baykara, S. (2020). What is PCI DSS and PCI Compliance?. Available at: https://pcidssguide.com/what-is-pci-dss-and-pci-compliance/ (Accessed: 9 June 2022).

Best Practice Certification Pty Ltd. (2021). What Are The Three Main Pillars Of Information Security?. Available at: https://bestpractice.biz/what-are-the-three-main-pillars-of-information-security/ (Accessed: 12 February 2022).

Bhandari, P. (2020). What Is Qualitative Research? | Methods & Examples. Available at: https://www.scribbr.com/methodology/qualitative-research/ (Accessed: 6 August 2023).

Bhandari, P. (2021). Correlation vs. Causation | Difference, Designs & Examples. Available at: https://www.scribbr.com/author/pritha/page/3/#:~:text=Published%20on%20July%207%2C%202021,two%20(or%20more)%20variables (Accessed: 6 August 2023).

Bhardwaj, P. (2019). Types of Sampling in Research. Journal of the Practice of Cardiovascular Sciences, Vol 5, Issue 3, pp. 157-163 Bhat, A. (2024). Exploratory Research: Types & Characteristics. Available at: https://www.questionpro.com/blog/exploratoryresearch/#:~:text=The%20main%20disadvantage%20of%20exploratory,interpreted%20for%20a%20genera lized%20population. (Accessed: 02 March 2024).

Bhatia, S., Behal, S., and Ahmed, I. (2018). Distributed Denial of Service Attacks and Defense Mechanisms: Current Landscape and Future Directions. In *Advances in Information Security* (Vol. 72, Issue December). https://doi.org/10.1007/978-3-319-97643-3_3

BioMelbourne Network. (2020). Importance of acceptable use policy – IT Systems & Services. Available at: https://biomelbourne.org/importance-of-acceptable-use-policy-it-systems-services/ (Accessed: 10 November 2021).

Biswas, P. (2020). Example of Physical Security Policy and Environmental Security Policy. Available at: https://isoconsultantkuwait.com/2020/02/01/example-of-physical-security-policy/ (Accessed: 11 November 2021). Blankenship, B. (2021). 5 Steps to Creating a Cybersecurity Incident Response Plan. Available at: https://blog.procircular.com/5-steps-to-creating-a-cybersecurity-incident-response-plan (Accessed: 10 November 2021).

Bonime-Blanc, A. and Saban,T. (2021). The 5 'Ts' of cyber-crisis readiness for every kind of organization. Available at: https://www.weforum.org/agenda/2021/09/cybersecurity-cyber-crisis-readiness/ (Accessed: 11 November 2021). Boru, T. (2018). CHAPTER FIVE RESEARCH DESIGN AND METHODOLOGY 5 . 1 . Introduction Citation : Lelissa TB (2018); Research Methodology ; University of South Africa , PHD Thesis. December. https://doi.org/10.13140/RG.2.2.21467.62242

Borza, M. (2021). Cyber Security Is Everyone's Responsibility. Available at: https://www.advantio.com/blog/cyber-security-is-everyones-responsibility (Accessed: 10 February 2022).

Braga, G. (2020). COBIT 2019 and the IIA 2019 Guiding Principles of Corporate Governance: Two Frameworks, Many Similarities. Available at: https://www.isaca.org/resources/news-and-trends/industrynews/2020/cobit2019-and-the-iia-2019-guiding-principles-of-corporate-governance (Accessed: 10 June 2022). Braun, V., and Clarke, V. (2006). Using thematic analysis in psychology; In qualittaive research in psychology. *Uwe Bristol*, *3*(2), 77–101. https://psychology.ukzn.ac.za/?mdocs-file=1176

Breiding, M. J. (2014). 肌肉作为内分泌和旁分泌器官 HHS Public Access. *Physiology and Behavior*, *63*(8), 1–18.

Bresnahan, E. (2023). The NIST Cybersecurity Framework Implementation Tiers Explained. Available at:

https://www.cybersaint.io/blog/the-nist-cybersecurity-framework-implementation-tiers-explained (Accessed: 18 April 2022).

Brooks, C. (2021). Cybersecurity Threats: The Daunting Challenge Of Securing The Internet Of Things. Available at: https://www.forbes.com/sites/chuckbrooks/2021/02/07/cybersecurity-threats-the-daunting-challengeofsecuring-the-internet-of-things/#:~:text=According%20to%20The%20McKinsey%20Global,security%20standards%20on%20the%20devices (Accessed: 22 October 2021).

Buchanan, R. (2019). *What We Know about Identity Theft and Fraud Victims from Research-and Practice-Based Evidence CENTER for VICTIM RESEARCH Research Report*. *August*, 34. https://ncvc.dspacedirect.org/bitstream/handle/20.500.11990/1544/CVR Research Syntheses_Identity Theft and Fraud_Report.pdf?sequence=1andisAllowed=y

Buckbee, M. (2021). Solving The Cybersecurity Skills Shortage Within Your Organization. Available at: https://www.varonis.com/blog/cybersecurity-skills-shortage (Accessed: 13 November 2021).

Budnik, k and Kirkwood, k. (2021). Building a united front on financial crimes in the financial services sector. https://www.pwc.co.za/en/press-room/cyber-security.html

businesstech.co.za. (2016). Watch out for these deposit and refund scams in South Africa. Available at: https://businesstech.co.za/news/finance/131176/watch-out-for-these-deposit-and-refund-scams-insouthafrica/ (Accessed: 10 October 2021).

businesstech.co.za. (2019). International investigation into cryptojacking in South Africa. Available at: https://mybroadband.co.za/news/security/303442-international-investigation-into-cryptojacking-insouthafrica.html (Accessed: 10 October 2021).

businesstech.co.za. (2020). These are the most common banking scams in South Africa. Available at: https://businesstech.co.za/news/banking/409869/these-are-the-most-common-banking-scams-insouthafrica/ (Accessed: 10 October 2021).

businesstech.co.za. (2021). Beware these 3 mobile threats in South Africa. Available at: https://businesstech.co.za/news/software/528538/beware-these-3-mobile-threats-in-south-africa/ (Accessed: 18 October 2021).

businesstech.co.za. (2021). Mimecast Report: 85% of SA organisations were hurt by lack of cyber preparedness in 2020. Available at: https://businesstech.co.za/news/industry-news/485419/mimecast-report-85-ofsaorganisations-were-hurt-by-lack-of-cyber-preparedness-in-2020/ (Accessed: 19 October 2021).

businesstech.co.za. (2021). These are the banking scams you should look out for in South Africa right now – with fraud on the rise. Available at: https://businesstech.co.za/news/banking/506418/these-are-thebankingscams-you-should-look-out-for-in-south-africa-right-now-with-fraud-on-the-rise/ (Accessed: 17 October 2021).

Business Optimization Training Institute. (2024). HOW TO BECOME ISO CERTIFIED IN SOUTH AFRICA. Available at: https://www.boti.co.za/how-to-become-iso-certified-in-south-africa/ (Accessed: 22 February 2024).

Business Process Incubator. (2020). What are the Benefits of COBIT 2019?. Available at: https://www.businessprocessincubator.com/content/what-are-the-benefits-of-cobit-2019/ (Accessed: 13 June 2022).

Cadmus Group Llc. (2019). Cybersecurity Preparedness Evaluation Tool. Available at: https://pubs.naruc.org/pub/3B93F1D2-BF62-E6BB-5107-E1A030CF09A0 (Accessed: 15 January 2022).

Carnal, D. (2023). 5 ways cyberattacks can damage a company's reputation. Available at: https://www.anapaya.net/blog/5-ways-cyberattacks-can-damage-a-companys-reputation (Accessed: 16 April 2024).

Center for Internet Security. (2021). *CIS Critical Security Controls, Version 8*. 59. Available at: https://www.cisecurity.org/controls/v8 (Accessed: 6 August 2023). Chamlou,

N. (2022). Why Diversity in Cybersecurity Matters. Available at:

https://www.cyberdegrees.org/resources/diversity-in-cybersecurity/ (Accessed: 15 April 2023).

Charter College. (2023). What Are the 3 Pillars of Cyber Security?. Available at: https://chartercollege.edu/newshub/what-are-3-pillars-cyber-security/ (Accessed: 12 February 2022).

Chase, E. (2021). CUSTOMER CYBERSECURITY AWARENES –CREATING A CULTURE OF SECURITY. Available at: https://sbscyber.com/resources/customer-cybersecurity-awareness-creating-a-cultureofsecurity (Accessed: 12 February 2022).

Chellappan, K., Mustafa, A. S., Mohammed, M. J., and ... (2015). Layered defense approach: towards total network security. *International Journal of …*, *December*. https://www.academia.edu/download/53472343/504-1490-1-PB.pdf

Chigada, J.M. (2020). A qualitative analysis of the feasibility of deploying biometric authentication systems to augment security protocols of bank card transactions. South African Journal of Information Management, 22(1), 1-9. https://dx.doi.org/10.4102/sajim.v22i1.1194

Chigada, J.M. (2023). Towards an aligned South African National Cybersecurity Policy Framework. Available at: https://open.uct.ac.za/items/4926b6ec-09eb-4abb-a23e-eb9170775fab

Chigada, J.M. and Daniels, N. (2021). Exploring information systems security implications posed by BYOD for a financial services firm. Business Information Review, 38(3), 115-126. https://doi.org/10.1177/02663821211036400

Chigada, J.M. and Kyobe, M. (2018). Evaluating Factors Contributing to Misalignment of the South African National Cybeersecurity Policy Framework. *International Conference on Information Resources Management (CONF-IRM)*, *November*.

Chigada, J.M. and Madzinga, R. (2021). Cyberattacks and threats during COVID-19 : A systematic literature review Coronavirus Disease-2019. 1–11.

Chipeta, C. (2022). What is the Cyber Threat Landscape?. Available at: https://www.upguard.com/blog/cyberthreat-landscape (Accessed: 31 July 2022).

Ciancaglini, V., Gibson, C. and Sancho, D. (2020). Malicious Uses and Abuses of Artificial Intelligence. Available at: https://documents.trendmicro.com/assets/white_papers/wp-malicious-uses-and-abuses-ofartificialintelligence.pdf (Accessed: 2 November 2023).

Cibangu, S.K. (2012). Qualitative Research: The Toolkit of Theories in the Social Sciences, IntechOpen, pp. 96 117.

Cin, P.D. and Jurgens, J. (2023). Global Cybersecurity Outlook 2023. Available at: https://www3.weforum.org/docs/WEF_Global_Security_Outlook_Report_2023.pdf (Accessed: 6 August 2023).

Cisco Systems, Inc. (2023) . What Is Phishing?. Available at: https://www.cisco.com/c/en/us/products/security/email-security/what-is-phishing.html (Accessed: 17 September 2023) Cisco Systems, Inc. (2023) . What Is Network Segmentation?. Available at: https://www.cisco.com/c/en/us/products/security/what-is-network-segmentation.html (Accessed: 17 September 2023).

Clark, E. (2020). THENIST CYBERSECURITY FRAMEWORK IMPLEMENTATION TIERS (PART 2OF 3). Available at: https://blog.twinstate.com/cybersecurity/nist/cybersecurity-framework-tiers (Accessed: 15 June 2022) Clements, C. (2020). The current state of consumers' cybersecurity awareness. Available at: https://www.securitymagazine.com/articles/92796-the-current-state-of-consumers-cybersecurity-awareness (Accessed: 12 February 2022).

Cohanim, A. (2023). The 5 steps to Building Cyber Skills and Readiness with KSA&Ts. Available at: https://www.cyberbit.com/icl-2023/the-5-steps-to-building-cyber-skills-and-readiness-with-ksats-not-sats/ (Accessed: 16 April 2024).

Collard, A. (2021). *Top IT security threats in 2021 Remote working security*. https://www.bizcommunity.com/Article/196/661/212269.html. (Accessed: 31 December 2021). Contracts Counsel, Inc. (2023). Acceptable Use Policy. Available at: https://www.contractscounsel.com/t/us/acceptable-use-policy (Accessed: 10 November 2021).

Coos, A. (2019). 5 Best Practices for PCI DSS Compliance. Available at:

https://www.endpointprotector.com/blog/5-best-practices-for-pci-dss-compliance/ (Accessed: 9 June 2022).

Crellin, C. (2015). 7 Ways To Increase Your Customers' Awareness Of Cybersecurity. Available at: https://www.mspinsights.com/doc/ways-to-increase-your-customers-awareness-of-cybersecurity-0001

(Accessed: 12 February 2022). Crocetti, P. (2021). What is data protection and why is it important?.

Available at:

https://www.techtarget.com/searchdatabackup/definition/data-protection?vgnextfmt=print (Accessed: 6 August 2023).

Crossman, A. (2019). Pilot Study in Research. Available at: https://www.thoughtco.com/pilot-study-3026449 (Accessed: 24 May 2021).

Currentware. (2023). How to Ensure Compliance With Policies and Procedures. Available at: https://www.currentware.com/blog/5-ways-to-enforce-your-acceptable-use-polic y/ (Accessed: 10 November 2021).

Cyber Law Consulting Centre. (2021). Bot Virus Dissemination. Available at: https://www.cybercrimechambers.com/blog-botvirus-dissemination--124.php (Accessed: 18 October 2021).

Cybersecurity and Infrastructure Security Agency. (2021). What is Cybersecurity?. Available at: https://www.cisa.gov/ncas/tips/ST04-001 (Accessed: 30 January 2021).

Cybersecurity and Infrastructure Security Agency. (2022). Weak Security Controls and Practices Routinely Exploited for Initial Access. Available at: https://www.cisa.gov/news-events/cybersecurityadvisories/aa22137a (Accessed: 12 February 2022).

CyberWarrior. (2023). We Need More Women in Cybersecurity. Available at: https://www.cyberwarrior.com/women-incybersecurity/ (Accessed: 30 July 2023).

Dallaway, E. (2016). Closing the Gender Gap in Cybersecurity. Available at: https://ngocc.org.zm/wp-content/uploads/2020/10/CREST-Closing-the-Gender-Gap-in-CyberSecurity.pdf (Accessed: 29 July 2023).

Danby, S. (2023). The ITIL 4 Service Value System Explained. Available at: https://itsm.tools/the-itil-4servicevalue-system-explained/#:~:text=%E2%80%9CA%20guiding%20principle%20is%20a,work%2C%20or%20management%20structure.%E2%80%9D (Accessed: 6 August 2023).

Daswani, N. and Elbayadi, M. (2021). 4 tips to help CISOs get more C-suite cybersecurity buy-in. Available at: https://www.techtarget.com/searchsecurity/post/4-tips-to-help-CISOs-get-more-C-suite-cybersecuritybuyin?vgnextfmt=print (Accessed: 31 July 2023).

Dataprise. (2023). Trends Among Cyber Insurance Companies + A Cyber Insurance Checklist. Available at: https://www.dataprise.com/resources/blog/cyber-insurance-exclusions/

De Groot, J. (2019). What is PCI Compliance?. Available at: https://digitalguardian.com/blog/what-pci-compliance (Accessed: 27 October 2021).

de Jager, M., Futcher, L., and Thomson, K.L. (2023). An Investigation into the Cybersecurity Skills Gap in South Africa. In: Furnell, S., Clarke, N. (eds) Human Aspects of Information Security and Assurance. HAISA 2023. IFIP Advances in Information and Communication Technology, vol 674. Springer, Cham. https://doi.org/10.1007/978-3-031-38530-8_19

Deloitte. (2019). Understanding phishing techniques Understanding phishing techniques Overview. December.

Device Authority. (2024). Security and Privacy Issues in IoT Generated Big Data. Available at: https://deviceauthority.com/security-and-privacy-issues-in-iot-generated-big-data/ (Accessed: 13 April 2024).

Dhamdhere, M., Karande, S., and Phatak, M. (2017).

Peer Group Analysis in Identity and Access Management to Identify Anomalies, International Journal of Latest Trends in Engineering and Technology, Vol.(8)Issue(1), pp.300-308 DOI: http://dx.doi.org/10.21172/1.81.039 e-ISSN:2278-621X

Dlamini, S. (2020). Data breach at Experian, 24 million South Africans' personal information exposed. Available at:https://www.iol.co.za/business-report/companies/data-breach-costs-sa-companies-r402million-average-in2020-6649ae0a-b803-482c-978f-b395517c7fa7 (Accessed: 13 October 2021).

Dlamini, S., Mbambo, C., and Ma, W.W.K. (2019).
Understanding policing of cybe-rcrime in South Africa : The phenomena , challenges and effective responses Cogent Social Sciences, 5(1).https://doi.org/10.1080/23311886.2019.1675404

Dolley, C. (2021). Cyberattacks: South Africa, you've been hacked. Available at: https://www.dailymaverick.co.za/article/2021-11-06-cyberattacks-south-africa-youve-been-hacked/ (Accessed: 12 February 2022).

Domains.co.za. (2020). SPAM ALERT: South Africa is under attack!. Available at: https://www.domains.co.za/blog/spam-alertsouth-africa-is-under-attack.html (Accessed: 10 October 2021).

Donston-Miller, D. (2021). Why Your Organization Should Have an Email Security Policy. Available at: https://www.mimecast.com/blog/why-your-organization-should-have-an-email-security-policy/ (Accessed: 10 November 2021).

Dosal, B. (2023). Effects of Cybercrime for Business: the Hidden Costs. Available at: https://www.compuquip.com/blog/effects-of-cybercrime-for-business-the-hidden-costs (Accessed: 6 August 2023).

Doyle, K. (2022). The top threats of 2022 (and how to fight them). Available at: https://www.itweb.co.za/content/mYZRX79gmj3qOgA8 (Accessed: 22 October 2022).

Dror, N. (2021). Top 5 Security Threats Facing Artificial Intelligence and Machine Learning. Available at: https://hubsecurity.io/top-5-security-threats-facing-artificial-intelligence-and-machine-learning/ (Accessed: 29 October 2021).

Dudovskiy, J. (2022). The Ultimate Guide to Writing a Dissertation in Business Studies: A Step-by-Step Assistance (6th edition). Availalble at: https://research-methodology.net/about-us/ebook/ (Accessed: 28 August 2022).

Dusane, P. S. and Pavithra, Y. (2020). Logic bomb: An insider attack. *International Journal of Advanced Trends in Computer Science and Engineering*, *9*(3), 3662–3665. https://doi.org/10.30534/ijatcse/2020/176932020

Eastwood, J., Ettema, R., Souza, D., Liu, H., Busetto, L., Ben, H., Patrick, H. and Schrijvers, G. (2018). Realist Research Design and Evaluation for Integrated Care RIC SIG - Part 1: Establishing a Special Interest Group. International Journal of Integrated Care,18(S2): A255, pp. 1-8. , DOI: dx.doi.org/10.5334/ijic.s2255

Edmead, M.T. (2020). Using COBIT 2019 to Plan and Execute an Organization's Transformation Strategy. Available at: https://www.isaca.org/resources/news-and-trends/industry-news/2020/using-cobit-2019-toplanand-execute-an-organization-transformation-strategy (Accessed: 13 June 2022).

Eldredge, J. D., Weagel, E. F. and Kroth, P. J. (2014). Population : CTSA-Affiliated Faculty Members. *National Institute of Health*, *26*(1), 5–11.

Ellis, R. (2019). How COBIT Relates to Risk Management. Available at: https://medium.com/@reciprocitymarketingoutreach/how-cobit-relates-to-risk-management-af748e6a17f1 (Accessed: 13 June 2022). Elue, E. (2020). Effective Capability and Maturity Assessment Using COBIT 2019. Available at: https://www.isaca.org/resources/news-and-trends/industry-news/2020/effective-capability-and-maturityassessment-using-cobit-2019 (Accessed: 10 June 2022).

Ervural, B. C. and Ervural, B. (2018). *Overview of Cyber Security in the Industry 4.0 Era*. *September 2018*, 267–284. https://doi.org/10.1007/978-3-319-57870-5_16

Etikan, I. and Bala, K. (2017). Sampling and Sampling Methods. *Biometrics and Biostatistics International Journal*, *5*(6), 215– 217. https://doi.org/10.15406/bbij.2017.05.00149

Exabeam. (2022). The 12 PCI DSS Requirements Explained. Available at: https://www.exabeam.com/explainers/pci-compliance/the-12-pci-dss-requirements-explained/ (Accessed: 9 June 2022).

F-Secure. (2023). Trojan-Downloader. Available at: https://www.f-secure.com/v-descs/trojan-downloader.shtml (Accessed: 18 October 2021).

F-Secure. (2023). Trojan-Proxy. Available at: https://www.f-secure.com/v-descs/trojan-proxy.shtml (Accessed: 18 October 2021).

Flick, U. (2014). The SAGE Handbook of Qualitative Data Analysis. London: SAGE Publications Ltd. Available at: <https://doi.org/10.4135/9781446282243> (Accessed: 5 August 2023).

FINANCIAL APPLICATION. (2018).

Fleming, J. and Zegwaard, K.E. (2018). Methodologies, methods and ethical considerations for conducting research in work-integrated learning. International Journal of Work-Integrated Learning, v19, n3, pp. 205213

Fortinet, Inc. (2023). What Is UEBA?. Available at:

https://www.fortinet.com/resources/cyberglossary/whatisueba#:~:text=UEBA (Accessed: 3 September

2023). Fortinet, Inc. (2023). What Is Vishing and a Vishing Attack?. Available at:

https://www.fortinet.com/resources/cyberglossary/vishing-attack (Accessed: 18 October 2021).

Fox, N. (2022). What is an Incident Response Plan and How to Create One. Available at: https://www.varonis.com/blog/incident-response-plan (Accessed: 10 November 2021).

Friend, D. (2022). Why you should escape from cloud vendor lock-in. Available at: https://technative.io/whyyoushould-escape-from-cloud-vendor-lock-in/ (Accessed: 27 August 2022).

Froner, K. (2018). Critical Paradigm Theory: A Deconstruction of the Dominant Discourse Shaping Public Education in America: City University of New York, 2018

Fruhlinger, J. (2020). The CIA triad: Definition, components and examples. Available at: https://www.csoonline.com/article/568917/the-cia-triad-definition-components-and-examples.html

(Accessed: 21 August 2021). Fruhlinger, J. (2022). PCI DSS explained: Requirements, fines, and

steps to compliance. Available at:

https://www.csoonline.com/article/569591/pci-dss-explained-requirements-fines-and-stepstocompliance.html (Accessed: 9 June 2022).

FTI Consulting Inc.. (2020). In South Africa, Cybersecurity Investments are Needed Amid COVID-19 Pandemic. Available at: https://www.fticonsulting.com/insights/articles/south-africa-cybersecurity-investmentsneededamid-covid-19-pandemic (Accessed: 19 October 2021).

Gallager, P. (2020). What are the Benefits of COBIT 2019?. Available at: https://blog.goodelearning.com/subjectareas/cobit/what-are-the-benefits-of-cobit-2019/ (Accessed: 13 June 2022).

Gañán, C. H., Ciere, M. and Van Eeten, M. (2017). Beyond the pretty penny: The Economic Impact of Cybercrime. *ACM International Conference Proceeding Series*, 35–45. https://doi.org/10.1145/3171533.3171535

Ganguly, S. (2023). 7 IoT Security Issues and How To Prevent Them. Available at: https://www.designrush.com/agency/software-development/trends/iot-securityissues#:~:text=Without%20any%20authorization%2C%20users%20are,data%2C%20breaking%20the%20 network%20perimeter (Accessed: 13 April 2024).

Gcaza, N. and von Solms, R. (2017). *A National Strategy for a Cybersecurity Culture: A South African Perspective*. 1–17. https://doi.org/10.1002/j.1681-4835.2017.tb00590.x

George, T. (2022). Semi-Structured Interview | Definition, Guide & Examples. Available at: https://www.scribbr.com/methodology/semi-structured-interview/

Geskey, J. M., Erdman, H. J., Bramley, H. P., Williams, R. J. and Shaffer, M. L. (2012). Superior mesenteric artery syndrome in intellectually disabled children. *Pediatric Emergency Care*, *28*(4), 351–353. https://doi.org/10.1097/PEC.0b013e31824d9bc5.

Global Forum on Cyber Expertise. (2023). Critical Information Infrastructure Protection Initiative. Available at: https://thegfce.org/initiative/critical-information-infrastructure-protection-initiative/ (Accessed: 15 September 2023).

Global Information Security Workforce Study. (2021). A Resilient Cybersecurity Profession Charts the Path Forward. *International Information System Security Certification Consortium*, *2021*, 1–43. https://www.isc2.org/-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx

Glover, G. (2023). What are the 12 requirements of PCI DSS Compliance?. Available at: https://www.securitymetrics.com/blog/what-are-12-requirements-pci-dss-compliance (Accessed: 9 June 2022 throughout 2023).

GoJ. (2015). Cybersecurity Strategy (Provisional Translation). Available at: http://www.nisc.go.jp/active/kihon/pdf/cybersecuritystrategy-en.pdf (Accessed: 10 September 2021).

González-Granadillo, G., González-Zarzosa, S. and Diaz, R. (2021). Security information and event management (SIEM): Analysis, trends, and usage in critical infrastructures. *Sensors*, *21*(14). https://doi.org/10.3390/s21144759

Goodman, S., Cole, K., Chetty, M., Larosa, C., Rietta, F., Schmitt, D. K. and Goodman, S. E. (2015). *Cybersecurity in Africa : An Assessment Cybersecurity in Africa : An Assessment*. *February*.

Goodspeed, L. (2022). PCI DSS v4.0 Resource Hub. Available at: https://blog.pcisecuritystandards.org/pci-dssv40-resource-hub

Gordon, L.A., Loeb, M.P. and Zhou, L. (2020). Integrating cost–benefit analysis into the NIST Cybersecurity Framework via the Gordon–Loeb Model, Journal of Cybersecurity, Volume 6, Issue 1, tyaa005, https://doi.org/10.1093/cybsec/tyaa005

Graham, K. (2021). Cybersecurity Readiness: What Is It and How Do You Evaluate Yours?. Available at: https://www.bitsight.com/blog/cybersecurity-readiness (Accessed: 10 February 2022).

Graham, K. (2023). Cybersecurity Readiness (Definition and 4 Evaluation Steps). Available at: https://www.bitsight.com/blog/cybersecurity-readiness (Accessed: 16 April 2024).

Grobler, R. (2020). Former Cape Town barman gets 5 years for cloning customers' bank cards. Available at: https://www.news24.com/news24/SouthAfrica/News/former-cape-town-barman-gets-5-years-for-cloningcustomers-bank-cards-20200819.

Heath, C. (2023). What is snowball sampling?. Available at: https://dovetail.com/research/snowball-sampling/ (Accessed: 29 July 2023).

Halder, S. (2021). What is NIST Cybersecurity Framework? (CSF) | Complete Guide. Available at: https://www.appknox.com/blog/nist-cybersecurity-framework (Accessed: 9 June 2022).

Hammer, A. (2024). Understanding information security governance. Available at: https://www.readynez.com/en/blog/understanding-information-security-governance/ (Accessed: 17 April 2024).

Hanna, K.T. (2022). What is ISO 27001?. Available at: https://www.techtarget.com/whatis/definition/ISO27001?vgnextfmt=print (Accessed: 6 August 2023).

Harmony Solutions ltd. (2019). What's So Amazing About COBIT 2019?. Available at: https://www.linkedin.com/pulse/whats-so-amazing-cobit-2019-harmony-solutions-ltd/?trk=article-ssrfrontend-pulse_more-articles_related-content-card (Accessed: 10 June 2022).

Hartwig, B. (2021). How Companies Can Increase Cybersecurity Awareness Among Their Employees. Available at: https://trainingmag.com/how-companies-can-increase-cybersecurity-awareness-among-theiremployees/ (Accessed: 10 February 2022).

Hasham, S. Joshi, S. and Mikkelsen, D. (2019). Financial crime and fraud in the age of cybersecurity. Available at: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/financial-crime-and-fraud-in-the-age-of-cybersecurity (Accessed: 12 October 2021). Hayes, A. (2022). Systematic Sampling: What Is It, and How Is It Used in Research?. Available at: https://www.investopedia.com/terms/s/systematic-sampling.asp (Accessed: 15 April 2023).

Helixstorm. (2023). HOW TO CREATE A MOBILE DEVICE MANAGEMENT POLICY: 9 BEST PRACTICES. Available: https://www.helixstorm.com/blog/how-to-create-a-mobile-device-management-policy/ (Accessed: 10 November 2021 throughout 2023).

Henke, C. (2023). What Is IoT Security? Risks, Examples, and Solutions. Available at: https://www.emnify.com/iot-glossary/iot-security (Accessed: 10 March 2024).

Houle, C., and Pandey, R. (2018). A layered approach to defending against list-linking email bombs. *ECrime Researchers Summit, ECrime*, *2018-May*, 1–9. https://doi.org/10.1109/ECRIME.2018.8376214

Hovarth, I. (2021). The Differences Between COBIT 5 and COBIT 2019. Available at:

https://www.invensislearning.com/blog/cobit-5-vs-cobit-2019/ (Accessed: 10 June 2022).

Hu, S. (2014). Encyclopedia of Quality of Life and Well-Being Research. Available at: https://link.springer.com/referenceworkentry/10.1007%2F978-94-007-0753-5_2256

Huang, K., Wang, X., Wei, W., and Madnick, S. (2023). The Devastating Business Impacts of a Cyber Breach. Available at: https://hbr.org/2023/05/the-devastating-business-impacts-of-a-cyber-breach (Accessed: 29 July 2023).

Hughes, C. (2022). Using the NIST Cybersecurity Framework to address organizational risk. Available at: https://www.csoonline.com/article/571911/using-the-nist-cybersecurity-framework-to-addressorganizationalrisk.html (Accessed: 9 June 2022).

Hussain, A. and Cheng, M. (2022). What Is Identity Theft? Definition, Types, and Examples. Available at: https://www.investopedia.com/terms/i/identitytheft.asp (Accessed: 24 July 2022).

IGI Global. (1988-2023). What is Information Security Ecosystem. Available at: https://www.igiglobal.com/dictionary/integrative-framework-study-information-security/14484 (Accessed: 13 February 2022).

Imperva. (2023). Insider Threat. Available at: https://www.imperva.com/learn/application-security/insider-threats/

(Accessed: 29 October 2021 throughout 2023). InfoSec Insights. (2021). What Is Cyber Security All About? 13

Experts Weigh In.

https://sectigostore.com/blog/what-is-cyber-security-all-about-experts-weigh-in/

In, J. (2017). Introduction of a pilot study. *Korean Journal of Anesthesiology*, *70*(6), 601–605. https://doi.org/10.4097/kjae.2017.70.6.601

Independent Online. (2021). South Africans urged to stay alert of cybercrime. Available at: https://www.iol.co.za/personal-finance/my-money/banking/south-africans-urged-to-stay-alert-ofcybercrime-5558fd31-caf5-4afd-9ac1-cf07399733e5 (Accessed: 19 October 2021).

Industry, P. C., and Procedures, T. (2022). *Payment Card Industry Data Security Standard Requirements and Testing Procedures*. *March*.

Innovation, I. (2019). Digital Innovation Profile: South Africa. ITU Innovation, 79(5), 1–24.

InstantSecurityPolicy.com. (2022). CONFIDENTIAL DATA POLICY. Available at:

https://www.instantsecuritypolicy.com/defs-confidential_data_policy.html (10 November 2021).

Intelligent CIO. (2019). Number of users attacked by banking Trojans grew by 16%. Available at: https://www.intelligentcio.com/africa/2019/03/11/number-of-users-attacked-by-banking-trojans-grew-by-16/ (Accessed: 18 October 2021).

Intellesec. (2021). The top 5 biggest cyber threats to your business in 2021. Available at: https://intellesec.co.uk/top-5-cyber-threats-2021/ (Accessed: 31 Dcember 2021).

International Information System Security Certification Consortium (ISC) 2 . (2019). Strategies for Building and Growing Strong Cybersecurity Teams. (ISC)2 Cybersecurity Workforce Study, 2019, 1–37. International Information System Security Certification Consortium (ISC) 2 Global Information Security Workforce Study. (2021). A Resilient Cybersecurity Profession Charts the Path Forward. Available at: https://iapp.org/resources/article/isc2-2021-cybersecurity-workforce-study/ (Accessed: 29 July 2023).

International Telecommunication union. (2018;2019;2020). Definition of cybersecurity. Available at: https://www.itu.int/en/ITUT/studygroups/com17/Pages/cybersecurity.aspx#:~:text=Cybersecurity%20is%20the%20collection%20of,a nd%20organization%20and%20user's%20assets. (Accessed: 5 April 2021).

Interpol. (2023). INTERPOL report shows alarming rate of cyberattacks during COVID-19. Available at:

https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-ofcyberattacks-during-COVID-19 (Accessed: 16 October 2021).

Irwin, L. (2021). 4 powerful benefits of PCI DSS compliance. Available at: https://www.itgovernance.eu/blog/en/4powerful-benefits-of-pci-dss-compliance (Accessed: 9 June 2022).

Ismail, N., Kinchin, G. and Edwards, J.-A. (2017). Pilot Study, Does It Really Matter? Learning Lessons from Conducting a Pilot Study for a Qualitative PhD Thesis. International Journal of Social Science Research, 6(1), 1. https://doi.org/10.5296/ijssr.v6i1.11720

IT Governance. (2021). ITIL ® v3 to ITIL ® 4 What has changed and how to transition. Available at: https://www.itgovernance.eu/en-ie/itil-v3-to-itil-v4-what-has-changed-ie (Accessed: 14 June 2022).

IT Governance. (2023). Cyber Security Risk Assessments (10 Steps to Cyber Security). Available at: https://www.itgovernance.asia/cyber-security-risk-assessments-10-steps-to-cyber-security (6 August 2023).

IT Pillars. (2024). Security Impact of IoT – Risks and Challenges. Available at: https://www.it-pillars.com/blog/securityimpact-of-iot/#:~:text=That's%20the%20security%20impact%20of,our%20little%20gadget%20friends%20lack (Accessed: 13 April 2024).

IT-Online. (2013). Managing mobile security in South Africa. Available at: https://itonline.co.za/2013/06/24/managing-mobilesecurity-in-south-africa/ (Accessed: 10 November 2021).

ITWeb Limited. (2022). SA records massive jump in impersonation attacks. Available at: https://www.itweb.co.za/content/WnxpE74YDGeMV8XL (Accessed: 28 August 2022).

ITWeb Security Summit. (2022). New research: budget pinch undermining organisations' ability to protect against cyber threats. Available at: https://www.itweb.co.za/content/DZQ58vV8VN4MzXy2 (Accessed: 30 July 2023).

ITWeb Security Summit. (2023). What makes SA a target for cyber crime, what actions can be taken?. Available at: https://www.itweb.co.za/article/what-makes-sa-a-target-for-cyber-crime-what-actions-can-betaken/Pero37Z34ydMQb6m (Accessed: 16 April 2024). Jackson, A. (2023). Cyber attack increase across Africa threatens digital growth. Available at: https://cybermagazine.com/cyber-security/cyber-attack-increase-across-africa-threatens-digital-growth (29 July 2023).

Jerzewski, M. (2022). CIS Control 15: Service Provider Management. Available at: https://securityboulevard.com/2022/02/cis-control-15-service-provider-management/ (Accessed: 15 June 2022)

Jerzewski, M. (2022). CIS Control 16 Application Software Security. Available at: https://securityboulevard.com/2022/04/ciscontrol-16-application-software-security/ (Accessed: 15 June 2022).

Kaput, M.B. (2023). What Can Happen to a Company as the Result of Cybercrime?. Available at: https://smallbusiness.chron.com/can-happen-company-result-cybercrime-26811.html (Accessed: 6 August 2023).

Kaspersky Lab. (2021). What is Smishing and How to Defend Against it. Available at: https://www.kaspersky.com/resource-center/threats/what-is-smishing-and-how-to-defend-against-it (Accessed: 18 October 2021).

Katrenko, A. (2004-2021). Cloud Computing Attacks: A New Vector for Cyber Attacks. Available at: https://www.apriorit.com/dev-blog/523-cloud-computing-cyber-attacks (Accessed: 24 October 2021).

Kaushik, V., and Walsh, C. A. (2019). Pragmatism as a research paradigm and its implications for Social Work research', Social Sciences, 8(9). doi: 10.3390/socsci8090255.h paradigm and its implications for Social Work research. Social Sciences, 8(9), 1–17.

Kavanagh, S. and Sharif, TA. (2021). African Cyberthreat Assessment Report. Available at: https://www.interpol.int/content/download/16759/file/AfricanCyberthreatAssessment_ENGLISH.pdf

Khadka, I. (2015). *Software piracy: A study of causes, effects and preventive measures*. *January*, 60.

https://www.theseus.fi/bitstream/handle/10024/87274/Khadka_Ishwor.pdf?sequence=1

Khaleefa, E. J. and Abdulah, D. A. (2022). Concept and difficulties of advanced persistent threats (APT): Survey. *International Journal of Nonlinear Analysis and Applications*, *13*(1), 4037–4052. https://ijnaa.semnan.ac.ir/article_6230.html

Kidd, C. (2019). What is COBIT? COBIT Explained. Available at: https://www.bmc.com/blogs/cobit/ (Accessed: 31 May 2022).

Kiger, M. E. and Varpio, L. (2020). Thematic analysis of qualitative data: AMEE Guide No. 131. *Medical Teacher*, *42*(8), 846–854. https://doi.org/10.1080/0142159X.2020.1755030

Knowledgehut Solutions Private Limited. (2023). ITIL®4 Guiding Principles. Available at: https://www.knowledgehut.com/tutorials/itil4-tutorial/itil-guiding-principles (Accessed: 6 August 2023).

Knowledgehut Solutions Private Limited. (2023). ITIL V3 vs ITIL V4: What's The Difference. Available at: https://www.knowledgehut.com/blog/it-service-management/itil-v4-vs-itil-v3

koigi, B. (2020). South Africa has third-highest number of cybercrime victims globally, report. Available at: https://africabusinesscommunities.com/tech/tech-news/south-africa-has-third-highest-numberofcybercrime-victims-globally-report/at: (Accessed: 12 February 2022).

Korstjens, I. and Moser, A. (2018). Series: Practical guidance to qualitative research. Part 4: Trustworthiness and publishing. *European Journal of General Practice*, *24*(1), 120–124. https://doi.org/10.1080/13814788.2017.1375092 Kosten, S. (2020). 7 Cloud Computing Security Vulnerabilities and What to Do About Them. Available at: https://towardsdatascience.com/7-cloud-computing-security-vulnerabilities-and-what-to-doabout-theme061bbe0faee (Accessed: 27 August 2022). KPMG. (2018). BUILDING CYBER RESILIENCE IN ASSET MANAGEMENT. Available at: https://assets.kpmg.com/content/dam/kpmg/uk/pdf/2018/04/building-cyber-resilience-inassetmanagement.pdf (Accessed: 6 August 2023).

KPMG. (2018). Cyber Insurance – How Insuretechs Can Unlock The Opportunity. Available at: https://assets.kpmg.com/content/dam/kpmg/za/pdf/2017/12/17383MC-cyber-insurance.pdf (Accessed: 11 November 2021)

Kraska, P. B., Brent, J. J. and Neuman, W. L. (2020). Qualitative Research and Analysis. *Criminal Justice and Criminology Research Methods*, 333–362. https://doi.org/10.4324/9780429026256-11

krishnan, J. (2023). Password Policy Recommendations for Sysadmins in 2023. Available at: https://www.securden.com/blog/top-10-password-policies.html (29 July 2023).

Krunal, O. (2023). Web Jacking. Available at: https://www.scribd.com/document/472092466/Web-Jacking (Accessed: 18 September 2023).

Laaser, U. and Beluli, F. (2016). "Special Volume 2016, A Global Public Health Curriculum (2nd Edition)", South Eastern European Journal of Public Health (SEEJPH). doi: 10.4119/seejph-1828.

Laubscher, E. (2018). Unskilled labour in South Africa. Available at: https://medium.com/@erichlaubscher1/unskilled-labour-in-south-africa-af56852ed443 (Accessed: 24 July 2022).

Lazic, M. (2023). 39 Worrying Cyber Crime Statistics [Updated for 2023]. Available at: https://legaljobs.io/blog/cyber-crime-statistics/ (Accessed: 9 November 2021).

Learningcurve. (2017). South African Companies hit hard for pirated software. Available at: https://learningcurve.co.za/southafrican-companies-hit-hard-for-pirated-software/ (Accessed: 13 October 2021).

Lecturer, S. (2018). research paradiagms_Perera. 2018(August).d

Ledesma, J. (2022). What is an APT?. Available at: https://www.bitdefender.com/blog/businessinsights/what-isanapt/ (Accessed: 3 September 2023).

Lindsey, N. (2019). ATM Malware and Jackpotting Attacks Could Be Making a Return. Available at: https://www.cpomagazine.com/cyber-security/atm-malware-and-jackpotting-attacks-could-be-makingareturn/ (29 October 2021).

Lotter, D. (2019). EXPLAINER: 3 ways to protect your business from cyber attacks. Available at: https://www.news24.com/fin24/opinion/explainer-3-ways-to-protect-your-business-from-cyberattacks20190720

Lucid Software Inc. (2023). Best practices for ITIL capacity management. Available at: https://www.lucidchart.com/blog/itil-capacity-management-service-design (Accessed; 6 August 2023).

Luz Yolanda Toro Suarez. (2015). *The main focus of the sense of health is the center of the household and the high-income people at home. The analysis of the co-dispersion structure of health-related indicators is titled. 1–27.*

Mabuza, E. (2020). Data breach: Experian identifies files, criminal case under investigation. Available at: https://www.timeslive.co.za/news/south-africa/2020-09-02-data-breach-experian-identifies-filescriminalcase-under-investigation/ (Accessed: 17 October 2021).

Maccoll, J., Nurse, J.R.C. and Sullivan, J. (2021). Cyber Insurance and the CyberSecurity Challenge. Available at: https://rusi.org/explore-our-research/publications/occasional-papers/cyber-insurance-and-cyber-securitychallenge (Accessed: 11 November 2021).

MacKay, J. (2024). How Do Hackers Get Caught and Exposed?. Available at: https://www.metacompliance.com/blog/phishing-and-ransomware/how-do-hackers-normally-getcaught#:~:text=Hackers%20will%20often%20use%20secure,layers%20to%20mask%20their%20identity (Accessed: 16 April 2024).

Maguire, M. and Delahunt, B. (2017). Doing a Thematic Analysis: A Practical, Step-by-Step Guide for Learning and Teaching Scholars.*, Journal of Teaching and Learning in Higher Education (AISHE-J), Volume 8, Number, pp. 3351-33514

Mahajan, A., and Sharma, S. (2015). The Malicious Insiders Threat in the Cloud. *International Journal of Engineering Research and General Science*, *3*(2), 246–256. www.ijergs.org

Moyo, A. (2016). Standard Bank hit by R300m fraud. Available at: https://www.itweb.co.za/article/standard-bank-hit-by-r300m-fraud/x4r1lyMRmxw7pmda (Accessed: 24 July 2022).

Moyo, A. (2021). SA-based debt collector hit by massive ransomware attack. Available at: https://www.itweb.co.za/article/sa-based-debt-collector-hit-by-massive-ransomwareattack/Pero3qZxjPD7Qb6m (Accessed: 19 October 2021).

Malatji, M. and Marnewick, A. L. (2021). *Cybersecurity Policy and the Legislative Context of the Water and Wastewater Sector in South Africa*. Sustainability 2021, 13, 291. https://doi.org/10.3390/ su13010291.

Malinga, S. (2021). Absa fires, lays criminal charges against data leak employee. Available at: https://www.itweb.co.za/content/DZQ58MVPYyovzXy2 (Accessed: 24 July 2022).

Malone, K. (2020). NIST Shares Cybersecurity Framework Implementation Tips. Available at: https://www.meritalk.com/articles/nist-shares-cybersecurity-framework-implementation-tips/ (9 June 2022).

Manship, R. (2022). The Top 6 Industries At Risk For Cyber Attacks. Available at: The Top 6 Industries At Risk For Cyber Attacks - RedTeam Security (Accessed: 31 July 2023).

Mathenge, M. J. and Stevens-Hall, J. (2019). ITIL 4 Management practices [Online]. Available at: https://www.bmc.com/blogs/itil-management-practices/ (Accessed: 31 May 2022).

Matters, W. R. (2016). INFORMATION SECURITY IN BANKS AND FINANCIAL.

Mcanyana, W., Brindley, C., and Seedat, Y. (2020). *Insight into the cyberthreat landscape in South Africa*.

McCombes, S. (2019). Sampling Methods | Types, Techniques and Examples. Available at: https://www.scribbr.com/methodology/sampling-methods/#:~:text=Probability (Accessed: 15 April 2023).

McLean, M. (2023). 2023 Must-Know Cyber Attack Statistics and Trends. Available at:

https://www.embroker.com/blog/cyber-attack-statistics/ (Accessed: 15 April 2023).

Meharchandani, D. (2020). 7 Cloud Vulnerabilities Endangering Your Data!. Available at: https://kratikal.com/blog/cloud-vulnerabilities/ (Accessed: 27 August 2022).

Microsoft. (2018). What businesses should be doing to mitigate cyber security risks. Available at: https://www.itweb.co.za/content/O2rQGqApK9ZMd1ea (Accessed: 10 October 2021). Milkovski,

I. (2021). Physical Security System Components. Available at:

https://www.linkedin.com/pulse/physical-security-system-components-igor-milkovski-ma (Accessed: 15

October 2023). Mokoka, M. (2020). SA is more cybersecure than it was a year ago, but it's still vulnerable.

Available at:

https://www.news24.com/citypress/news/sa-is-more-cybersecure-than-it-was-a-year-ago-but-its-stillvulnerable-20200306#google_vignette (Accessed: 19 October 2021).

Morano, J. (2023). NIST CSF 2.0: What you need to know. Available at: https://blog.quest.com/nist-csf-2-0whatyou-need-to-know/

Morse, J.M., Barrett, M., Mayan, M., Olson, K. and Spiers, J. (2002). Verification Strategies for Establishing Reliability and Validity in Qualitative Research Janice. *Advances in Experimental Medicine and Biology*, *812*(2), 325–331. https://doi.org/10.1007/978-1-4939-0620-8_43

Morris, M. (2021). 9 Advantages of Cybersecurity Risk Assessment. Available at: https://www.sdtek.net/9advantages-of-cybersecurity-risk-assessment (Accessed: 6 August 2023).

Moyo, A. (2019). Bad day for SA's cyber security as banks suffer DDoS attacks. Available at: https://www.itweb.co.za/content/LPp6V7r4OVzqDKQz (Accessed: 24 July 2022).

Moyo, A. (2020). Public cloud services under cyber security threat in SA. Available at: https://www.itweb.co.za/content/JN1gPvOYkl3MjL6m (Accessed: 24 October 2021).

Munthe-Kaas, H., Nøkleby, H., Lewin, S. and Glenton, C. (2020). The TRANSFER Approach for assessing the transferability of systematic review findings. *BMC Medical Research Methodology*, *20*(1), 1–22. https://doi.org/10.1186/s12874-019-0834-5

Mwita, K. (2022). Strengths and weaknesses of qualitative research in social science studies, International Journal of Research in Business and Social Science 11(6)(2022), pp. 618-625. : https://www.ssbfnet.com/ojs/index.php/ijrbs.

NCPF. (2015). The National Cybersecurity Policy Framework (NCPF) For South Africa - 2015. *Government Gazette*, *39475*, 1–30. http://www.gov.za/sites/www.gov.za/files/39475_gon609.pdf

Netwrix Corporation. (2023). Password Policy Best Practices for Strong Security in AD . Available at: https://www.netwrix.com/password_best_practice.html (Accessed: 11 November 2021 throughout 2023).

Nexus Group. (2024). What Are The Security Challenges of IoT?. Available at: https://www.nexusgroup.com/what-are-the-security-challenges-of-iot/ (Accessed: 13 April 2024).

Ngulube, P. (2015). Qualitative data analysis and interpretation: systematic search for meaning. *Addressing Research Challenges: Making Headway for Developing Researchers*, *June*, 131–156. https://doi.org/10.13140/RG.2.1.1375.7608

Nguyen-Duy, J. (2018). How Digital Transformation Has Impacted Security and How to Minimize Risk. Available at: https://www.csoonline.com/article/3292927/how-digital-transformation-has-impactedsecurity-and-how-tominimize-risk.html (Accessed: 19 October 2021).

Nikolopoulou, K. (2022). What Is Non-Probability Sampling? | Types & Examples. Available at: https://www.scribbr.com/methodology/non-probability-sampling/ (6 August 2023).

Nowell, L. S., Norris, J. M., White, D. E. and Moules, N. J. (2017). Thematic Analysis: Striving to Meet the Trustworthiness Criteria. International Journal of Qualitative Methods, 16(1), 1–13.

https://doi.org/10.1177/1609406917733847

Nweke, L.O. (2017). Using the CIA and AAA Models to Explain Cybersecurity Activities. PM World Journal, Vol. VI, Issue XII, pp. 1-3

Nyasvisvo, B. and Chigada, J. M. (2023) "Phishing Attacks: A Security Challenge for University Students Studying Remotely," The African Journal of Information Systems: Vol. 15: Iss. 2, Article 3. Available at: https://digitalcommons.kennesaw.edu/ajis/vol15/iss2/3 O'dea, B. (2021). How to solve the cybersecurity workforce shortage. Available at: https://www.siliconrepublic.com/careers/how-to-solve-the-cybersecurity-workforce-shortage (Accessed: 13 November 2021).

Ochieng, J. (2023). 11 Critical Items for a Network Security Policy. Available at: https://cyberexperts.com/network-security-policy/ (Accessed: 18 October 2023).

Office for the Coordination of Humanitarian Affairs. (2016). What is preparedness?. Available at: https://www.humanitarianresponse.info/en/coordination/preparedness/what-preparedness (Accessed: 10 February 2022).

Olcott, J. (2016). COBIT Vs. ITIL: Which Framework Works Best For Cybersecurity?. Available at: https://www.bitsight.com/blog/cobit-vs-itil (Accessed: 6 August 2022).

Oltsik, J. (2021). 7 key data points on the cybersecurity skills shortage. Available at: https://www.csoonline.com/article/571189/7-key-data-points-on-the-cybersecurity-skills-shortage.html (Accessed: 13 November 2021).

Openpath, Inc. (2021). Physical Security Guide. Available at: https://www.openpath.com/physical-security-guide (Accessed: 11 November 2021).

Osborne, C. (2020). Absa bank embroiled in data leak, rogue employee accused of theft. Available at: https://www.zdnet.com/article/absa-bank-embroiled-in-data-leak-rogue-employee-accused-of-theft/ (Accessed: 15 January 2021)

Palo Alto Networks. (2023). What is an IT Security Policy?. Available at: https://www.paloaltonetworks.com/cyberpedia/what-is-an-it-security-policy#:~:text=The%20objectives%20of%20an%20IT,of%20assets%20from%20unauthorized%20entities (6 August 2023).

Palmer, D. (2021). The cybersecurity jobs crisis is getting worse, and companies are making basic mistakes with hiring. Available at: https://www.zdnet.com/article/the-cybersecurity-jobs-crisis-is-getting-worseandcompanies-are-making-basic-mistakes-with-hiring/ (Accessed: 30 October 2021).

Park, Y.S., Konge, L. and Artino, A.R. (2019). The Positivism Paradigm of Research. Academic Medicine, Vol. 95, No. 5, pp. 690-694. doi: 10.1097/ACM.0000000000003093. PMID: 31789841. Patel, N. (2021). The 8 Biggest Security Threats and Challenges for IoT. Available at: https://www.business2community.com/tech-gadgets/the-8-biggest-security-threats-and-challenges-for-iot02431222 (Accessed: 22 October 2021).

Payment Card Industry Security Standards Council. (2018). PCI DSS Quick Reference Guide Understanding the Payment Card Industry Data Security Standard version 3.2.1. Available at: https://listings.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf (Accessed: 9 June 2022).

Pervin, N. and Mokhtar, M. (2022). The Interpretivist Research Paradigm: A Subjective Notion of a Social Context. *International Journal of Academic Research in Progressive Education and Development*, *11*(2), 419–428. https://doi.org/10.6007/ijarped/v11-i2/12938

Pinnock, B. (2020). What recent data breaches tell us about cybersecurity in South Africa. Available at: https://businesstech.co.za/news/industry-news/433797/what-recent-data-breaches-tell-usaboutcybersecurity-in-south-africa/ (Accessed: 19 October 2021).

Prior, B. (2020). The most common banking scams of 2020. Available at: https://mybroadband.co.za/news/banking/379566the-most-common-banking-scams-of-2020.html (Accessed: 10 October 2021).

Pritz, A. (2021). Forbes: The Five-Step Recipe For Avoiding Insider Threat Disasters. Available at: https://www.revealrisk.com/forbes-the-five-step-recipe-for-avoiding-insider-threat-disasters/ (Accessed: 29 October 2021).

Putnam, L.L. and Banghart, S. (2017). Interpretive Approaches. Available at: https://www.researchgate.net/publication/314711771_Interpretive_Approaches (Accessed: 2 November 2023). PwC. (2023). Systems failure is a significant business risk. Available at: https://www.pwc.co.uk/issues/crisis-and-resilience/systems-failure.html (Accessed: 30 July 2023).

Pygma Consulting. (2023). CYBERSECURITY GOVERNANCE IN SOUTH AFRICA: A PERSPECTIVE ON POLICY, LEGISLATION AND REGULATION. Availale at: https://pygmaconsulting.com/cybersecuritygovernance-in-south-africa-a-perspective-on-policy-legislationand-regulation/ (Accessed: 19 October 2021).

Qadir, S. and Quadri, S. M. K. (2016). Information Availability: An Insight into the Most Important Attribute of Information Security. *Journal of Information Security*, *07*(03), 185–194. https://doi.org/10.4236/jis.2016.73014

Qualys, Inc. (2023). CyberSecurity Asset Management (CSAM). Available at: https://www.qualys.com/apps/cybersecurity-asset-management/ (Accessed: 6 August 2023).

Radoini, A. (2020). Cyber-crime during the COVID-19 pandemic. Freedom from Fear, Volume 2020, Issue 16, Oct 2020, p. 6 - 10. https://doi.org/10.18356/5c95a747-en

Rane, S. (2022). What are the 12 requirements of PCI DSS Compliance?. Available at: https://www.controlcase.com/what-are-the-12-requirements-of-pci-dss-compliance/ (Accessed: 9 June 2022).

RangeForce. (2024). 5 Reasons to Strengthen Team Cyber Readiness with Hands-On Skills Development. Available at: https://www.rangeforce.com/blog/5-reasons-to-strengthen-team-cyber-readiness-withhands-on-skills-development (Accessed: 16 April 2024).

Reese, H. (2021). The cybersecurity skills gap persists for the fifth year running. Available at: https://www.techrepublic.com/article/the-cybersecurity-skills-gap-persists-for-the-fifth-year-running/ (Accessed: 13 November 2021).

Reguly, T. (2021). CIS Control 08: Audit Log Management. Available at: https://www.tripwire.com/state-of-security/cis-control-08 (Accessed: 15 June 2022).

Reguly, T. (2021). CIS Control 10: Malware Defenses. Available at: https://www.tripwire.com/state-of-security/cis-control-10 (Accessed: 15 June 2022).

Reguly, T. (2021). CIS Control 17: Incident Response Management. Available at: https://www.tripwire.com/state-of-security/cis-control-08 (Accessed: 15 June 2022). Reguly, T. (2022). CIS Control 17: Incident Response Management. Available at: https://securityboulevard.com/2022/04/cis-control-17-incident-response-management/ *Release* (Accessed: 15 June 2022).

Reciprocity. (2023). Who Needs PCI DSS Compliance?. Available at: https://reciprocity.com/resources/whoneedspci-dss-compliance/ (Accessed: 9 June 2022).

Richmond, C. (2017). Cybersecurity Readiness: How "At Risk" Is Your Organization?. Available at: https://www.business.att.com/content/dam/attbusiness/reports/cs-cybersecurity-readiness-whitepaper.pdf (Accessed: 10 February 2022).

Robison, K. (2021). Why companies are flocking to the cloud more than ever. Available at: https://www.businessinsider.com/cloud-technology-trend-software-enterprise-2021-2 (Accessed: 24 October 2021).

Roohparvar, R. (2019). The three pillars of cybersecurity. Available at: https://www.infoguardsecurity.com/thethree-pillars-of-cybersecurity/ (Accessed: 12 February 2022).

Rosenthal, M. (2021). Insider Threat Statistics You Should Know: Updated 2021. Available at: https://www.tessian.com/blog/insider-threat-statistics/ (Accessed: 29 October 2021).

Rouse, M. (2017). Network Security Policy. Available at:

https://www.techopedia.com/definition/29916/networksecurity-policy#:~:text=Techopedia (Accessed: 10 November 2021).

RSI Security. (2019). CHALLENGES WITH CLOUD ENCRYPTION. Available at: HTTPS://BLOG.RSISECURITY.COM/CHALLENGES-WITH-CLOUD-ENCRYPTION/#:~:TEXT=MOREOVER%2C%20ONE%20OF%20THE%20CLOUD,PERFECT%20SOLUTION%20FOR%20DATA%20SECURITY. (27 August 2022).

Sabu, C. (2023). How Digital Transformation Impacts Cybersecurity: An Overview. Available at: https://experionglobal.com/how-digital-transformation-impacts-cybersecurity/#:~:text=As%20organizations%20digitize%20their%20operations,becoming%20more%20sophisticated%20and%20damaging. 10 October 2023).

Safianu, O., Twum, F. and Hayfron-Acquah J.B. (2016). Information System Security Threats and Vulnerabilities: Evaluating the Human Factor in Data Protection. International Journal of Computer Applications, 143(5), 8–14. https://doi.org/10.5120/ijca2016910160

SAGE Publications Inc. (2016). Pretesting and Pilot Testing 101. 101–119.

Sanchez, A. (2021). The 12 PCI DSS Compliance Requirements. Available at: https://www.alertlogic.com/blog/the-12-pci-dss-compliance-requirements/ (Accessed: 9 June 2022).

SANS Institute. (2021). CIS Controls v8. Available at: https://www.sans.org/blog/cis-controls-v8/ (Accessed: 6 August 2023).

Sarker, I. H., Abushark, Y. B., Alsolami, F., and Khan, A. I. (2020). IntruDTree: A machine learning based cyber security intrusion detection model. *Symmetry*, *12*(5), 1–15. https://doi.org/10.3390/SYM12050754 Schrader, D. (2023). CIS Control 1: Inventory and Control of Enterprise Assets. Available at: https://blog.netwrix.com/2022/05/04/inventory-control-enterprise-assets/ (Accessed: 15 June 2022).

Schrader, D. (2023). CIS Control 4: Secure Configuration of Enterprise Assets & Software. Available at: https://blog.netwrix.com/2022/05/04/secure-configuration-enterprise-assets-software/ (Accessed: 15 June 2022).

Schultz, C. B. (2016). CYBERCRIME : AN ANALYSIS OF CURRENT LEGISLATION IN SOUTH AFRICA By Charlotte Beverly Schultz Submitted in partial fulfilment of the requirements for the degree LLM (Mercantile Law) Faculty of Law University of Pretoria Supervisor : S Papadopoulos Octobe. October.

Seemma, P.S., Nandhini, S. and Sowmiya, M. (2018). *Overview of Cyber Security*, International Journal of Advanced Research in Computer and Communication Engineering *November*. Vol. 7, Issue 11. https://doi.org/10.17148/IJARCCE.2018.71127

Seifried,K. (2020). Over 200 Documented Blockchain Attacks, Vulnerabilities and Weaknesses. Available at: https://cloudsecurityalliance.org/blog/2020/10/26/blockchain-attacks-vulnerabilities-and-weaknesses/ (Accessed: 29 October 2021).

Shah, N. and Farik, M. (2017). Ransomware-Threats, Vulnerabilities And Recommendations. INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 6, ISSUE 06, pp. 307-309

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

Shiff, L. (2021). Top 7 Business Benefits of IT Service Management. Available at: https://www.bmc.com/blogs/business-benefits-service-management/ (Accessed: 31 May 2022).

Shiff, L. (2021). Popular IT Service Management (ITSM) Frameworks. Available at: https://www.bmc.com/blogs/itsm-frameworks-popular/ (Accessed: 31 May 2022).

Singh, A. (2023). What is a Salami Attack and How to protect against it?. Available at: https://www.shiksha.com/online-courses/articles/salami-attack-how-to-protect-against-it/ (Accessed: 2 November 2023).

Sileyew, K.S. (2020). Research Design and Methodology. Cyberspace. IntechOpen. https://doi.org/10.5772/intechopen.85731.

Simplilearn Solutions. (2023). What is COBIT? Understanding the COBIT Framework [Updated]. Available at: https://www.simplilearn.com/what-is-cobit-significance-and-framework-rar309-article (Accessed: 15 May 2022 throughout 2023).

Singh, R. (2019). SAMPLING PROCEDURE AND TYPES OF SAMPLING. Available at: https://www.academia.edu/41929754/SAMPLING_PROCEDURE_AND_TYPES_OF_SAMPLING (Accessed: 13 November 20230.

Skelton, S. K. (2022). *Hiring and retention challenges in cyber security persist. Available at:* https://www.computerweekly.com/news/252515016/Hiring-and-retention-challenges-in-cyber-securitypersist?vgnextfmt=print (Accessed: 6 August 2023).

Smillie,S. (2019). Hackers give City of Joburg, banks until Monday to pay 'ransom'. Available at:

https://www.iol.co.za/saturday-star/news/hackers-give-city-of-joburg-banks-until-monday-to-payransom35957235

(Accessed: 19 October 2021).

Smith, C. (2021). Over half a billion rand lost in debit card scams in SA last year. Available at: https://www.news24.com/fin24/companies/over-half-a-billion-rand-lost-in-debit-card-scams-in-sa-lastyear20210929 (Accessed: 18 October 2021).

Smith, Z.M. and Lostri, E. (2020). The Hidden Costs of Cybercrime. Available at: https://www.mcafee.com/dech/consumer-corporate/newsroom/press-releases/pressrelease.html?news_id=6859bd8c-9304-4147bdab-32b35457e629 (01 November 2021).

Sobers, R. (2021). What Is Cryptojacking? Prevention and Detection Tips. Available at: https://www.varonis.com/blog/cryptojacking (Accessed: 19 October 2021). Sobers,

R. (2022). 166 Cybersecurity Statistics and Trends [updated 2022]. Available at:

https://www.varonis.com/blog/cybersecurity-statistics#:~:text=Recent%20security%20research%20suggests%20most,a%20part%20of%20their%20cult ure (Accessed: 10 October 2021). Sohail, A. (2023). How COBIT 2019 Framework can be used to improve IT Governance. Available at:

https://www.businessbeam.com/blog/cobit-2019/ (Accessed: 13 June 2022 throughout 2023).

Sahoo, N. (2021). Preparing for the ISO27001 Certification?. Available at: https://www.vistainfosec.com/blog/benefits-of-iso-27001-certification/ (Accessed: 31 May 2022).

SolarWinds Worldwide, LLC. (2022). Service Level Management. Available at: https://www.solarwinds.com/service-desk/use-cases/service-level-management (Accessed: 31 May 2022).

South African Banks Risks Information Centre. (2023). Cybercrime. Available at: https://www.sabric.co.za/stay-safe/cybercrime/ (Accessed: 16 October 2021).

South African Government. (2017). Deputy Minister John Jeffery: Media briefing on Cybercrimes and Cybersecurity Bill. https://www.gov.za/speeches/cybercrimes-and-cybersecurity-bill-19-jan-2017-0000# (Accessed: 10 October 2021).

Sprintzeal Americas Inc. (2023). Cybercrime Impacts On Business: 6 Major Effects. Available at: https://www.sprintzeal.com/blog/cybercrime-business-impacts (Accessed: 6 August 2023). *stable*.

(2022).

Stahl, N. A., and King, J. R. (2014). Expanding approaches for research: Understanding and using trustworthiness in qualitative research. Journal of Developmental Education, 44(1), 26–28.

Su, N. (2018). Positivist Qualitative Methods. In: The SAGE Handbook of Qualitative Business and Management Research Methods: History and Traditions. 55 City Road, London: SAGE Publications Ltd. pp. 17-31 Available at: <https://doi.org/10.4135/9781526430212> [Accessed 15 Nov 2023].

Subhani, A. (2023). Industries At Risk Of Cyberattacks. Available at: https://www.forbes.com/sites/forbestechcouncil/2023/02/28/industries-at-riskofcyberattacks/?sh=6e535fbd49e1 (Accessed: 29 July 2023).

Swoboda, A. (2021). CIS Control 09: Email and Web Browser Protections.

Available at: https://www.tripwire.com/state-of-security/cis-control-09 (Accessed: 15 June 2022).

Swoboda, A. (2021). CIS Control 14: Security Awareness and Skill Training. Available at: https://www.tripwire.com/state-of-security/cis-control-14 (Accessed: 15 June 2022).

Taherdoost, H. (2022). Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview. *Electronics (Switzerland)*, *11*(14). https://doi.org/10.3390/electronics11142181

TechAdvisory.org. (2023). BYOD security tips. Available at: https://www.techadvisory.org/2019/11/byodsecuritytips/dosal (Accessed: 10 November 2021).

Teimoor, R. A. (2019). *Ethical Hacking and Knowledge about Hacking*. *June*. Computer Department - Collage of Science – University of Sulaimani,Iraq. https://doi.org/10.13140/RG.2.2.17344.79362

Tenable, Inc. (2023). CIS Control 2: Inventory and Control of Software Assets. Available at: https://docs.tenable.com/security-center/CIS-CAS/Content/Controls/Basic/Control-2/Control-2.htm (Accessed: 15 June 2022).

Terry, I. (2022). The Top 5 Cybersecurity Challenges Facing Financial Service Institutions. Available at: https://www.ispartnersllc.com/blog/top-5-cybersecurity-challenges-facing-financial-service-institutions/ (Accessed: 31 July 2023). Thames, L. (2021). CIS Control 13: Network Monitoring and Defense. Available at: https://www.tripwire.com/state-of-security/cis-control-13 (Accessed: 15 June 2022).

The Economic Times (2023). What is 'Trojan'. Available at: https://economictimes.indiatimes.com/definition/trojan (Accessed: 18 October 2021).

The Phoenix Group of Companies. (2023). Confidential Data Policy. Available at: https://www.phoenixlitho.com/privacy-policy/ (Accessed: 18 October 2023).

Thomas, A., 2020. Cybercrime : Types and Implications for Financial Institutions 3–7. Available at: https://medium.com/@netsentries/cybercrime-types-and-implications-for-financial-institutions263313b498b2 (Accessed: 12 October 2021).

Thomas, L. (2023). Cluster Sampling | A Simple Step-by-Step Guide with Examples. Available at: https://www.scribbr.com/methodology/cluster-sampling/#:~:text=What (Accessed: 29 July 2023).

Thomas, M. (2019). A New COBIT Is in Town and I Really Like How It Looks. Available at: https://www.isaca.org/resources/news-and-trends/industry-news/2018/a-new-cobit-is-in-town-and-ireallylike-how-it-looks (Accessed: 10 June 2022).

Threatpost. (2023). The True Impact of Ransomware Attacks. Available at: https://threatpost.com/true-impact-of-ransomware-attacks/168029/ (Accessed: 22 October 2021).

TMB Managed IT Services. (2022). Why Is It So Hard To Catch Cybercriminals?. Available at: https://blog.tmb.co.uk/why-is-it-so-hard-to-catch-cyber-criminals Truth, T. H. E. U. (2019). *UNSPOKEN*. 1–32.

Tooping, S. (2024). Securing Industry: Navigating the Challenges of Industrial IoT Security. Available at: https://www.globalsign.com/en/blog/Challenges-industrial-iotsecurity#:~:text=Legacy%20System%20and%20Network%20Vulnerabilities,these%20systems%20were%20in%20development. (Accessed: 13 April 2024).

Tozzi, C. (2022). How Important Is an ITIL Certification in 2022?. Available at: https://www.itprotoday.com/it-operations/how-important-itil-certification-2022 (Accessed: 31 May 2022).

Tredger, C. (2023). Lack of skills, immature judicial system weaken SA's cyber security stance. Available at: https://www.itweb.co.za/article/lack-of-skills-immature-judicialsystem-weaken-sas-cyber-security-stance/LPwQ57IbNwkqNgkj (Accesed: 16 April 2024).

Tunggal, A.T. (2023). Why is Vendor Risk Management Important?. Available at:

https://www.upguard.com/blog/vendor-risk-management-important (Accessed: 10 February 2022 throughout 2023).

Tunggal, AT. (2023). How to Perform a Cybersecurity Risk Assessment (2023 Guide). Available at: https://www.upguard.com/blog/how-to-perform-a-cybersecurity-risk-assessment Accessed: 10 February 2022 throughout 2023).

Uddin, H., Ali, H. and Hassan, M.K. (2020). Cybersecurity Hazards and Financial System Vulnerability: A Synthesis of Literature (30 07, 2020). Available at SSRN: https://ssrn.com/abstract=3689162 or http://dx.doi.org/10.2139/ssrn.3689162

Upadhyay, N. (2020). Demystifying blockchain: A critical analysis of challenges, applications and opportunities. International Journal of Information Management, Volume 54, https://doi.org/10.1016/j.ijinfomgt.2020.102120

Utica University. (2020). Ten Ways Evolving Technology Affects Cybersecurity. Available at: https://programs.online.utica.edu/resources/article/ten-ways-evolving-technology-affects-cybersecurity (Accessed: 19 October 2021).

Uzado Compliance and Cybersecurity Services. (2021). The 5 Benefits of the NIST Cyber Security Framework. Available at: https://www.uzado.com/blog/the-5-benefits-of-the-nist-cyber-security-framework/ (Accessed: 10 June 2022).

V-Soft Consulting. (1997-2021). The Cybersecurity Readiness List to Protect Your Business Against Hackers.Available at: https://blog.vsoftconsulting.com/blog/the-cybersecurity-readiness-list-to-protectyourbusiness-against-hackers (Accessed: 10 February 2022).

Van Bon, J. (2019). ITIL® 4 – A Pocket Guide. Van Haren Publishing, 's-Hertogenbosch, www.vanharen.net.

Van Niekerk, B. (2017). An Analysis of Cyber-Incidents in South Africa. *The African Journal of Information and Communication*, *20*, 113–132. https://doi.org/10.23962/10539/23573

Venktess, K. (2017). Local IT on high alert after SA PCs hit by global virus. Available at: https://www.news24.com/fin24/tech/news/local-it-on-alert-after-sa-computers-infected-by-globalvirus20170515

Vicente, V. (2023). The 12 PCI DSS Compliance Requirements: What You Need to Know. Available at: https://www.auditboard.com/blog/pci-dss-requirements/ (Accessed: 9 June 2022 throughput 2023).

Vielberth, M. (2021). Security Information and Event Management (SIEM). Encyclopedia of Cryptography, Security and Privacy, https://doi.org/10.1007/978-3-642-27739-9_1681-1

Vigliarolo, B. (2021). NIST Cybersecurity Framework: A cheat sheet for professionals. Available at: https://www.techrepublic.com/article/nist-cybersecurity-framework-the-smart-persons-guide/ (Accessed: 15 June 2022).

Voses, M.S. (2019). 5 Tips on How Companies Can Prepare for Cyberattacks and Data Breaches. Available at: https://www.securitymagazine.com/articles/91367-tips-on-how-companies-can-prepare-for-cyberattacksand-data-breaches (Accessed: 10 February 2022).

Vumetric Inc. (2023). 5 Benefits Of PCI-DSS Compliance. Available at: https://www.vumetric.com/blog/5benefitsof-pci-dss-compliance/ (9 June 2022 throughout 2023)

Walker, A. (2020). Phishing and malware attacks rise as SA goes into COVID-19 lockdown. Available at: https://memeburn.com/2020/03/cyber-attacks-south-africa-lockdown/ (Accessed: 13 October 2021).

Wembly Partners. (2021). NIST, ISO, COBIT, ITIL – Which Cyber Framework Rules Them All?. Available at: https://www.wembleypartners.com/post/nist-iso-cobit-itil-which-cyber-framework-rules-them-all (Accessed: 10 June 2022).

Wenning, J. (2021). CIS Control 05: Account Management. Available at: https://www.tripwire.com/stateofsecurity/cis-control-05 (Accessed: 15 June 2022).

Wenning, J. (2021). CIS Control 11: Data Recovery. Available at: https://www.tripwire.com/state-ofsecurity/ciscontrol-11 (Accessed: 15 June 2022).

White, S.K. and Greiner, L. (2022). What is ITIL? Your guide to the IT Infrastructure Library. Available at: https://www.cio.com/article/272361/infrastructure-it-infrastructure-library-itil-definition-and-solutions.ht (Accessed: 31 May 2022).

Williams, G., Fourie, T. and Siyaya, S. (2021). The newly enacted Cybercrimes Act and what it means for South Africans. Available at: https://www.golegal.co.za/newly-enacted-cybercrimes-act/#:~:text=26%20Jul%202021&text=The%20Act%20criminalises%20the%20disclosure,address%20aspects%20pertaining%20to%20cybersecurity. (Accessed: 30 October 2021).

Winder, D. (2021). How to build cybersecurity into your digital transformation project. Available at: https://www.raconteur.net/risk-regulation/build-cybersecurity-into-digital-transformation (Accessed: 19 October 2021).

Wisdom, J. and Creswell, J. W. (2013). Integrating quantitative and qualitative data collection and analysis while studying patient-centered medical home models. Agency for Healthcare Reseach and Quality, 13-0028-EF, 1–5. https://doi.org/No. 13-0028-EF.

World Health Organization. (2020). WHO reports fivefold increase in cyber attacks, urges vigilance. https://www.who.int/news/item/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urgesvigilanceITo (Accessed: 15 January 2021).

Yanthan, N. (2023). Service Value System in ITIL 4 Explained in Detail. Available at: https://www.sprintzeal.com/blog/service-value-system (Accessed: 6 August 2023).

Yong, WK., Maizaitulaidawati Md., Husin, M. and Kamarudin, S. (2021). Understanding Research Paradigms: A Scientific Guide Journal of Contemporary Issues in Business and Government Vol. 27, pp. 5857-5865

Zerlang, J. (2022). The Pandemic's Lasting Effects: Are Cyber Attacks One Of Them?, Available at: https://www.forbes.com/sites/forbestechcouncil/2022/07/20/the-pandemics-lasting-effectsare-cyber-attacks-one-of-them/?sh=601d9ce2b76c (Accessed: 27 August 2022).

Zhang, A. (2020). ICS Information Security Assurance Framework 12. Available at: https://nsfocusglobal.com/icsinformation-security-assurance-framework-12/ (Accessed: 13 February 2022)

Zubair, A.M. (2023). Experimental Research Design-types and process. Available at: https://www.researchgate.net/profile/Ahsanul-Zubair-2 (Accessed: 2 November 2023).

APPENDICES

Appendix 1: Interview Questions

UNIVERSITY of the
WESTERN CAPE

Department of Information Systems,

Economic and Management Sciences Faculty.

Interview Questions

Information system security vulnerabilities: Implications for South African financial firms in Cape Town.

Researcher:

Sinoxolo Sisanda Hermanus

Email: 3564354@myuwc.ac.za

Cell: +27 60 589 5786

Questions:

The questions below are based on information systems security on the different financial firms in Cape Town. Please answer the following based on the experiences in your organisation.

1. How do the changes in technology increase risks to organizations ?
2. What do you think is the biggest threat to the financial firms?
3. In your understanding, what is cybersecurity/ information systems security?
4. What are the strategies do you use in your firm to protect systems?
5. What are the challenges that your company face when implementing the strategies of information systems security?
6. If you have experienced any attacks in your firm, please elaborate on the nature of the attack(s)
7. Please provide ways in which the attacks are addressed in your firm.
8. What are the losses to the company due to the mentioned attacks?
9. What recommendations would you provide to other firms to improve their information systems security controls in order to reduce information systems security vulnerabilities.

End of document

Appendix 2: Ethical Clearance Certificate

UNIVERSITY of the WESTERN CAPE

60 YEARS of hope, action & knowledge

20 October 2021

Ms S Hermanus
Information Systems
Faculty of Economic and Management Sciences

HSSREC Reference Number:	HS21/7/50
Project Title:	Information system security vulnerabilities: Implications for South African financial firms in Cape Town.
Approval Period:	**20 October 2021 – 20 October 2024**

I hereby certify that the Humanities and Social Science Research Ethics Committee of the University of the Western Cape approved the methodology, and amendments to the ethics of the above mentioned research project.

Any amendments, extension or other modifications to the protocol must be submitted to the Ethics Committee for approval.

Please remember to submit a progress report by 30 November each year for the duration of the project.

For permission to conduct research using student and/or staff data or to distribute research surveys/questionnaires please apply via:
https://sites.google.com/uwc.ac.za/permissionresearch/home

The permission letter must then be submitted to HSSREC for record keeping purposes.

The Committee must be informed of any serious adverse events and/or termination of the study.

Ms Patricia Josias
Research Ethics Committee Officer
University of the Western Cape

Director: Research Development
University of the Western Cape
Private Bag X 17
Bellville 7535
Republic of South Africa
Tel: +27 21 959 4111
Email: research-ethics@uwc.ac.za

NHREC Registration Number: HSSREC-130416-049

FROM HOPE TO ACTION THROUGH KNOWLEDGE.

Appendix 3: Consent Forms

Private Bag X17, Belville, 7535
South Africa
Tel: +27 (0) 21 959 3680
Fax: +27 (0) 21 959 3522
www.uwc.ac.za

University of the Western Cape
Faculty of Economic and Management Sciences
Department of Information Systems

Research Participant Consent Form: Interviews

Project Title:	**Information system security vulnerabilities: Implications for South African financial firms in Cape Town.**

Please tick Yes or No to each of the following

		Yes	No
1.	I confirm that I have read and understand the information sheet explaining the above research project and I have had the opportunity to ask questions about the project.		
2.	I understand that my participation is voluntary and that I am free to withdraw at any time without giving any reason and without there being any negative consequences.		
3.	I understand that should I not wish to answer any particular question or questions, I am free to decline.		
4.	I understand my responses and personal data will be kept strictly confidential. I give permission for members of the research team to have access to my anonymised responses. I understand that my name will not be linked with the research materials, and I will not be identified or identifiable in the reports or publications that result for the research.		
5.	I agree that the interview may be recorded		
6.	I agree for the data collected from me to be used in future research.		
7.	I agree to take part in the above research project.		

Name of Participant (*or legal representative*)	Date	Signature
Name of person taking consent	Date	Signature

Contact details of study supervisor:
Name: Professor Joel Chigada
University of the Western Cape
Department of Information Systems
Telephone: 021 959 2578
Email: jchigada@uwc.ac.za

NOTE: *This research project has received ethical approval from the Humanities & Social Sciences Research Ethics Committee of the University of the Western Cape, Tel. 021 959 4111, email: research-ethics@uwc.ac.za*

Appendix 4: Research Project Information Sheet: Interviews

Private Bag X17, Belville, 7535
South Africa
Tel: +27 (0) 21 959 3680
Fax: +27 (0) 21 959 3522
www.uwc.ac.za

Faculty of Economic and Management Sciences
Department of Information Systems

Research Project Information Sheet: Interviews

Project Title:	Information system security vulnerabilities: Implications for South African financial firms in Cape Town.

What is this study about?
I am Sinoxolo Sisanda Hermanus, a student completing Master of Commerce degree in Information Systems at the University of the Western Cape. I am currently conducting research on the implications for Information system security vulnerabilities among South African financial firms in Cape Town. I am conducting this study for academic purposes. Even so, the findings from this research may also be shared with the university authorities and publicised.

Why have I been chosen?
You have been chosen because as a person who works in the Information and Communications Technology department, you will be able to provide information on the information systems security vulnerabilities in your firm.

What will I be asked to do if I agree to participate?
This interview has few semi-structured questions and takes about 30 minutes to finish, should one agree to participate. One can still choose not to answer the questions if they do not want to.

Would my participation in this study be kept confidential?
To protect your confidentiality, will not be required to provide any personal details, such as your name, address, or identity number, company name. All other details such as your age, education, employment status, etc. are therefore anonymous. This will ensure that you remain unidentifiable in any reports or publications. The data collected will kept safe in the university premises and any online information will be protected with the relevant security processes and technologies.

What are the risks of this research?
By participating in this research process there is a risk of exposing of exposing sensitive information about the cyber-attacks your firm has experienced previously. The researcher will ensure that the questions asked do not reveal any information that is confidential to the organization.

What are the benefits of this research?
Findings from this research will help financial firms examine their readiness to address cybercrime to improve firm security and lower vulnerabilities. Furthermore, the study will assist in reviewing the current cybersecurity policies and ways to improve those, while also exploring the future possibilities of information systems security for firms to remain ready.

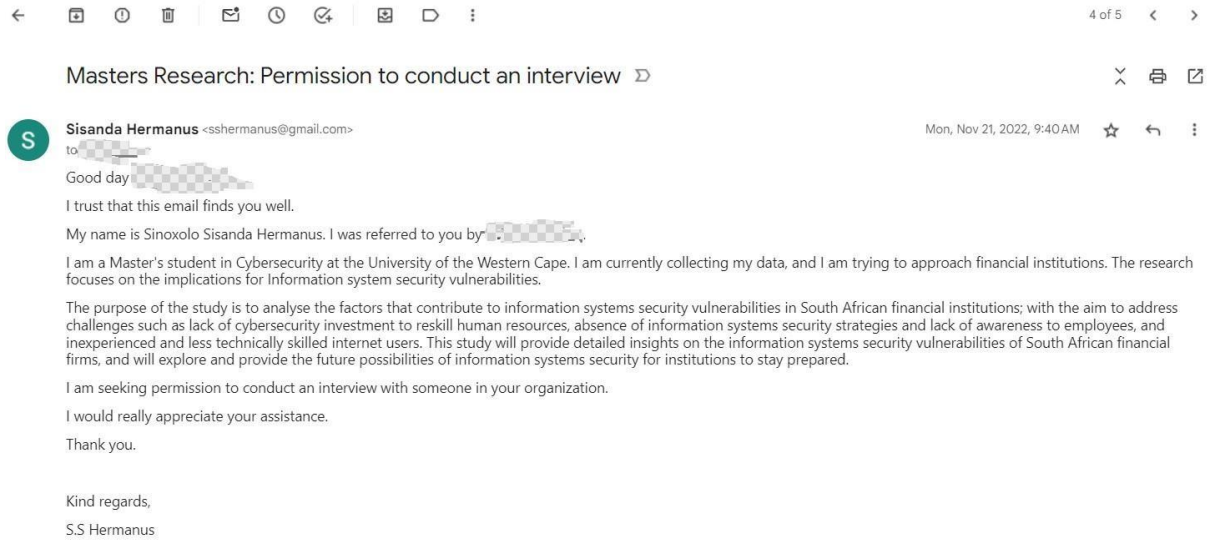
Do I have to be in this research, and may I stop participating at any time?
Your participation in this interview is completely and entirely voluntary. You may choose not to take part at all. If you decide to participate in this interview, you may stop participating at any time they want to.

What if I have questions?
If you have any questions feel free to contact the project leader:

Contact details of project leader (study supervisor)
Name: Professor Joel Chigada
University of the Western Cape, Department of Information Systems
Telephone: 021 959 2578
Email: jchigada@uwc.ac.za

Contact details of student
Name: Sinoxolo Sisanda Hermanus

Appendix 5: Email Seeking permission to conduct study



4 of 5

Masters Research: Permission to conduct an interview

Sisanda Hermanus <sshermanus@gmail.com> Mon, Nov 21, 2022, 9:40 AM
to

Good day

I trust that this email finds you well.

My name is Sinoxolo Sisanda Hermanus. I was referred to you by .

I am a Master's student in Cybersecurity at the University of the Western Cape. I am currently collecting my data, and I am trying to approach financial institutions. The research focuses on the implications for Information system security vulnerabilities.

The purpose of the study is to analyse the factors that contribute to information systems security vulnerabilities in South African financial institutions; with the aim to address challenges such as lack of cybersecurity investment to reskill human resources, absence of information systems security strategies and lack of awareness to employees, and inexperienced and less technically skilled internet users. This study will provide detailed insights on the information systems security vulnerabilities of South African financial firms, and will explore and provide the future possibilities of information systems security for institutions to stay prepared.

I am seeking permission to conduct an interview with someone in your organization.

I would really appreciate your assistance.

Thank you.

Kind regards,

S.S Hermanus