Developing a Cybersecurity Framework for Commercial Banks in South Africa

by

Tlhologelo Kweletsi Mphahlele

(Student No. 3342081)

Submitted in fulfilment of the requirements for the
degree of Doctor of Philosophy
in Information Systems

in the

Department of Information Systems

Economic and Management Sciences Faculty

at the

University of the Western Cape
Supervisor: Prof. J. Chigada

May 2023

DECLARATION

I, **Tlhologelo Mphahlele,** hereby declare that the work on which this thesis, ‘Developing a Cybersecurity Framework for Commercial Banks in South Africa,’ is my original work (except where acknowledgements indicate otherwise) and that neither the whole work nor any part of it has been, is being, or is to be submitted for another degree at this or any other university. I authorise the university to reproduce for the purpose of research either the whole or any portion of the contents in any manner whatsoever.

With the help and constructive guidance of the IS scholarly community, I have integrated and incorporated various ideas to develop this thesis.

“I also confirm that I have been granted permission by the University of the Western Cape’s Doctoral Degrees Board to include the following publications in my PhD thesis and where co-authorships are involved, my co-authors have granted me permission to include the publication”:

- Mphahlele, T.K. & Chigada, J. 2023. Mitigating cyber-attacks and in South African commercial banks, The African Journal of Information Systems, (Under review)

Signature: Date: 04 May 2023

Approved by supervisor

Date: 24 April 2023

Abstract

Cybersecurity has emerged as a significant concern for organisations and the Information Communication Technology (ICT) domain during recent decades. An increase in the number of cyber threats and cyber-attacks has been observed recently, and an even sharper increase was noticed during the worldwide coronavirus (COVID-19) pandemic outbreak. Simultaneously, the complexity of the cyber-attacks being executed by threat actors has increased, and the scope and geographical location of the targets of threat actors have also widened to include critical infrastructure in all corners of the world. Commercial banks in South Africa have not been spared. This is because financial institutions are seen as valuable targets by cybercriminals and communicators of advanced persistent threats (APT) due to the nature of their business and the vast amounts of data they store.

The study proposed a conceptual Cybersecurity Framework for Commercial Banks in South Africa. It proposed this by identifying the factors impeding commercial banks from developing their frameworks due to the challenges faced by the banks regarding cybersecurity from a South African perspective. The factors were identified using a mixed methods approach, with qualitative data collection facilitated through interviews with professionals within the banking domain in South Africa and quantitative data collected using a survey distributed to IT, risk, compliance, and governance professionals in commercial banks. The study identified seven factors contributing to establishing a cybersecurity framework for commercial banks. By addressing these factors, some of the challenges experienced by commercial banks regarding cybersecurity in the country can be addressed, which will improve the security posture of the organisations, internally and externally.

The study proposed that the stronger the coherence among the identified factors, the better commercial banks can defend themselves from cybercriminals. The findings further highlighted that for commercial banks to address the challenges posed by cybersecurity adequately, they would have to address cybersecurity holistically, placing equal emphasis on people, processes, and technology. They would also have to implement better security education, training, and awareness programmes for their employees and customers. In addition, commercial banks would have to bolster their capabilities for detecting and responding to cyber-attacks and collaborate more through establishing a national information sharing and analysis centre (ISAC). Furthermore, the study reinforced the need for commercial banks to invest in improving their cybersecurity detection, response, and remediation capabilities. Given the global shortage of skilled cybersecurity professionals, organisations should focus on developing talent internally through upskilling and breaking down barriers to entry into the cybersecurity domain.

Given the nature of cybersecurity and the sensitivity of the information associated with cybersecurity, the key limitation the researcher faced when conducting the study was a failure to obtain the necessary permissions to carry out the survey within the banks and to get first-hand accounts of previous incidents and how they were dealt with. During the study, it became evident that cybersecurity is a field that commercial banks and the South African government are still in the process of coming to grips with. Future research could investigate how well the cabinet's new laws and regulations have had the desired impact on cybercrimes and cyber threats within the country. Additionally, to gather a more comprehensive picture of the threats and patterns of bank attacks, further studies could focus on obtaining the necessary permissions and clearance to study cyber-attacks and threat actors within the banks. Due to its sensitivity, this will enable better data collection and access to information that is not publicly available. In addition, an investigation into how the frameworks within banks are developed to support cybersecurity may also be carried out.

Keywords: Advanced persistent threats, Cyber threats, Cyber-attacks, Cybersecurity, Cybersecurity frameworks, Threat actors.

Acknowledgements

All praise is due to the Almighty God, the Lord of Lords, who gave me the ability, strength, endurance, and guidance to complete this study. I express my deepest gratitude to my thesis supervisor, Professor Joel Chigada, for his advice, support, and encouragement throughout my research journey. His expertise, valuable insights, and constructive feedback have been instrumental in shaping my research work.

I owe a debt of gratitude to my wife, Kgaugelo Mphahlele, whose constant support, inspiration, and affirmation helped me stay motivated throughout my research journey, especially when I wanted to give up.

I want to extend my heartfelt thanks to my mother, Ramaredi Irene Mphahlele, who has been my constant inspiration and encouragement. Her unwavering support and kind words have always inspired me to reach goals I once thought were impossible. I am profoundly grateful for all her sacrifices to ensure I received the best education possible. I would also like to thank Sadie Flora Mphahlele, whose prayers kept me going during the challenging times of my academic journey. I am also grateful to all my other family members and friends who have encouraged me and shown their support throughout my journey. Your support and encouragement mean the world to me, and I am forever grateful for your kindness and generosity. I also sincerely thank the respondents, participants, and gatekeepers who made this research possible. Your contributions and support were essential to the success of this study.

Once again, thank you to everyone who made this research possible in their unique ways.

Table of Contents

Table of Figures

List of tables

List of abbreviations and acronyms

AGFI	Adjusted goodness-of-fit index
AI	Artificial Intelligence
APT	Advanced Persistent Threats
ATM	Automatic Teller Machine
BI	Business Intelligence
BYOD	Bring your own device
C2	Command and control
CABS	Community of African Banking Supervisors
CEH	Certified Ethical Hacker
CEO	Chief Executive Officer
CFA	Confirmatory factor analysis
CFI	Comparative fit index
CHFI	Computer Hacking Forensic Investigator
CIA	Confidentiality, Integrity and Availability
CIS	Centre for Internet Security
CISO	Chief Information Security Officer
CISSP	Certified Information Systems Security Professional
CMIN	Chi-squared Value
COVID	Coronavirus disease
CSIR	Council for Scientific and Industrial Research
CPMI-	Committee on Payments and Market Infrastructures and the International
IOSCO	Organisation of Securities Commission
CRI	Cyber Readiness Index
CSA	Certified SOC Analyst
CSF	Cybersecurity Framework
CSIR	Council for Scientific and Industrial Research
CSIRT	Computer Security Incident Response Teams
CVE	Common Vulnerabilities and Exposures
DDoS	Distributed Denial of Service

DF	Degrees of freedom
DLP	Data loss prevention
DMZ	Demilitarised zone
ECSP	Electronic Communications Service Provider
EDR	Endpoint detection and response
ENISA	European Union Agency for Cybersecurity
FSCA	Financial Sector Conduct Authority
GDPR	General Data Protection Regulation
GFI	Goodness-of-fit index
HB	Human Behaviour
HI	High Interval
IBM	International Business Machines
ICT	Information Communications Technology
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IFI	Incremental Fit Index
IG	Implementation Groups
IMF	International Monetary Fund
IOC	Indicators of compromise
IP	Internet Protocol
IPS	Intrusion Prevention System
ISAC	Information Sharing Analysis Centres
ISACA	Information Systems Audit and Control Association
ISC	International Information System Security Certification Consortium
ISMS	Information Security Management System
ISO	International Organisation for Standardization
IT	Information Technology
ITU	International Telecommunications Union
MitM	Man-in-the-middle
NA	National Assembly
NACS	Network Access Control

NCAC	National Cyber Security Advisory Council
NCOP	National Council of Provinces
NCPF	National Cybersecurity Policy Framework
NFI	Normal fit index
NIST	National Institute of Standards and Technology
NQF	National Qualifications
OWASP	Open Worldwide Application Security Project
PCI-DSS	Payment Card Industry Data Security Standard
PIN	Personal Identification Number
POPIA	Protection of Personal Information Act
POS	Points of Sale
R&D	Research and development
RFI	Relative fit Index
RMSEA	Root means square error of approximation
SA	South Africa
SABRIC	South African Banking Risk Information Centre
SANS	Sysadmin, Audit, Network and Security
SAPS	South African Police Service
SARB	South African Reserve Bank
SCCM	System Centre Configuration Manager
SETA	Security Education, Training and Awareness)
SMS	Short message service
SOC	Security Operations Centre
SP	Security posture
SQL	Structured query language
ST	Security training
STEM	Science, Technology, Engineering, and Mathematics
SWIFT	Society for Worldwide Interbank Financial Telecommunications
TA	Threat awareness
TCP	Transmission control protocol
TLI	Tucker-Lewis Index

TOGAF	The open group architecture framework
TTP	Techniques, tactics, and procedures
UDP	User datagram protocol
US	United States
USD	United States Dollar
WHO	World health organisation
XDR	Extended detection and response
XSS	Cross-site scripting
ZAR	South African Rand

List of equations

PART I

Chapter One : Introduction And Background

1.1 Introduction

With the advancements in Information Communication Technologies (ICTs), innovation has been seen across multiple industries by introducing services such as digital government, digital commerce, digital education, digital health, digital environment, and digital banking. These services have enabled commercial banks to reach more people without needing a physical locality. In the financial services industry, the development of Financial Technology (FinTech) in areas such as Mobile Internet, cloud computing, big data, search engines and blockchain technology has significantly changed the financial industry (Cheng, Li, Wu & Luo, 2017). However, the growth and adoption of online financial services have not come without drawbacks. Information technology systems continue to be plagued by cybersecurity breaches, which are rapidly increasing in complexity and severity, affecting economic interests, local and national security, and intellectual property (Tisdale, 2015). As cybercrimes have become more prevalent, financial institutions have become prime targets for criminals, as these institutions offer more significant attack vectors due to the increased number of services provided to their clients online, resulting in financial institutions increasingly becoming victims of cybercrimes.

As the ubiquity of digital banking and online financial services continues to rise, the need for a practical framework to handle the cybersecurity needs of financial institutions must ensure that both the institutions and their clients remain protected. The study analyses factors that impede the development of a practical cybersecurity framework, thus necessitating the development of a conceptual framework. The number of cybercrimes has drastically increased in South Africa in recent years. According to the South African Banking Risk Information Centre (SABRIC), the number of cybercrimes reported between January and August 2018 was 16,296 (van der Westhuizen, 2019). Cyber threats faced by financial institutions have varied tremendously and have increased in complexity during recent years, with institutions in South Africa not being exempt from threats, and the global pandemic (COVID-19) exacerbated increases in the number of threats faced by institutions (Chigada & Madzinga, 2021). Multiple local and international financial institutions have been targets of Distributed Denial of Service (DDoS) attacks, web attacks, cyber espionage, card skimming, phishing and attacks on Points of Sale (POS) terminals (Catota, Morgan & Sicker, 2018). It is becoming an ever-increasing challenge for South African institutions to protect their digital assets, detect breaches, and respond appropriately to identified threats, with institutions finding themselves in situations where they not only have to deal with usual operations but at the same time have to address the challenges that new ways of work (hybrid and remote) have placed on them. Ransomware has also gained a noticeable foothold locally, with multiple institutions falling victim to ransomware attacks (Mabunda, 2019).

The Cyber Readiness Index (CRI), which measures a nation's cyber readiness, employs seven elements to assess nations' readiness; these seven elements can be applied to financial institutions as they exist within nations and form part of critical infrastructure. They contribute to the overall security posture and cybersecurity maturity of nations. The seven elements of the CRI 2.0 are National strategy, Incident response, E-crime and law enforcement, Information sharing, Investment in research and development (R & D), Diplomacy and trade, and defence and crisis response. With the recent data breaches such as Nedbank's third-party service provider (Computer Services Ltd), ViewFines, Master Deeds, Momentum, and Liberty, to name a few, substantial amounts of personally identifiable information belonging to individuals were lost. This information now exists on the web and could potentially be used by criminals to further perpetrate crimes under the pretence of being connected with those institutions. These breaches caused the institutions to suffer considerable financial losses and reputational damage that sometimes could not be overcome (Zetter, 2015). The continued prevalence and effectiveness of cyber-attacks can be partially credited to an organisation's inability to detect potential cyber threats in the various phases before an attack. Lockheed Martin (2011) described the phases of an attack in the cyber kill chain framework: reconnaissance, weaponisation, delivery, exploitation, installation, command and control (C2), and actions on objectives. This inability to detect the preliminary phases may be attributed to limited time, a lack of soft skills (information dissemination), employee training, inadequate technology, and a lack of comprehension of the national laws around cybersecurity (SANS Institute, 2019). Managing an organisation's cybersecurity risks depends on understanding its business drivers and considering the security considerations specific to its use of technology. This occurs because every organisation's risks, priorities, and systems are unique to that organisation. The National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure for Cybersecurity lists five core functions that can be performed concurrently and continuously to form an operational culture that addresses dynamic cybersecurity risks (Barrett, 2018). They are Identify, Protect, Detect, Respond, and Recover. Using these five cores, an organisation should be able to manage the specific cybersecurity risks it is exposed to.

To employ successful information security, the three pillars of the information security triad must be satisfied: confidentiality, integrity, and availability. Confidentiality concerns access control around information and system permissions, and integrity concerns the authenticity of the information being viewed and accessed. The information accessed should be consistent throughout each stage of change. Availability refers to anyone authorised to access and modify information within an appropriate timeframe. When looking to secure information resources, organisations must balance the need for security with users' need to access and use these resources effectively (Bourgeios, Mortati, Wang & Smith, 2019).

Hathaway, Demchak, Kerben McArdle and Spidalieri (2015) defined cyber readiness as a 'state of maturity via a commitment to secure the cyberinfrastructure and services upon which the digital future and growth of the entity depend'. The CRI refers to a study undertaken by Hathaway *et al.* (2015) to examine one hundred and twenty-five countries that had embraced or were starting to embrace ICT. The study evaluated the countries' seven elements to determine their preparedness, maturity, and commitment to cyber security. The South African Cybercrimes Act [B6 of 2017], which came into effect in 2021, defined cybercrimes as unlawful access, unlawful interception of data, unlawful acts in respect of a software or hardware tool, illegal interference with data or computer programs, unlawful interference with a computer data storage medium or computer system, unlawful acquisition, possession, provision, receipt or use of a password, access code or similar data or device, cyber fraud, cyber forgery and discussion of same, cyber extortion, aggravated offences, and theft of incorporeal property (Department of Justice and Constitutional Development, 2016). The European Commission defines cybercrimes as online criminal acts using electronic communications networks and information systems. These crimes include online fraud and forgery, illegal online content, and crimes specific to the Internet, such as attacks against information systems or phishing (European Commission, 2007). The US Department of Justice further defines cybersecurity in a threefold definition: the first is crimes in which the computer or computer network is the target of the criminal activity, the second is existing offences where a computer is a tool used to commit the crime, and thirdly, being crimes in which the use of a computer is an incidental aspect of the commission of a crime, but may afford evidence of such crime (Clough, 2015).

1.2 Contextual Setting Of The Thesis

The setting of this study is cybersecurity within the commercial banking sector in South Africa, which comprises the central bank (South African Reserve Bank), five large local banks and other smaller banks and financial institutions. The sector is considered well-developed and is ranked relatively high compared to developed nations. In 2017, the South African banking sector ranked 11th out of 138 countries in market development in the Global Competitiveness Report. It also ranked 2nd out of 138 countries in terms of bank soundness. A sound banking system ensures the optimal allocation of capital resources and efficient management of risks to prevent costly banking system crises and their associated adverse feedback effects on the real economy (Schwab, 2019; Schwab, 2017) Simbanegavi, Greenberg and Gwatidzo (2015) stated that the South African banking sector is monopolistically competitive. However, this does not indicate a lack of efficiency or competitiveness within the market. Moyo (2018) further corroborated this by highlighting that the sector comprised 64 institutions in 2017, which indicates competitiveness. With 98 per cent of the market share concentrated among the big five banks, this indicates monopolistic competitiveness. In the fiscal year 2019 to 2020, the collective market share of the five big banks (Standard Bank, FirstRand, Absa, Nedbank, and Investec) reduced to 89.4 per cent of the total banking assets managed and controlled within the country, with local branches of foreign banks accounting for 7 per cent and other banks accounting for 3.6 per cent of the banking sector (South African Reserve Bank Prudential Authority, 2020). As of July 2023, the ranks of the five big banks have seen the entrance of Capitec. With Capitec replacing Investec in the ranks (Business Tech, 2023).

1.3 Definition Of Key Terms

This section of the chapter defines the key terms that informed the study:

Advanced persistent threats (APT): This is a type of threat actor in the top tier of sophistication and skill. Such actors can use advanced and zero-day techniques to carry out complex and protracted cybersecurity campaigns to pursue their goals (Canadian Centre for Cyber Security, 2022).

Cyber-attacks: Any malicious activity or action that attempts to collect, disrupt, deny, or destroy information systems' resources or the information itself of an organisation or individual (National Institute of Standards and Technology, 2019).

Cybercrime: Zhang, Yanping, Xiao, Ghaboosi, Zhang and Deng (2012) defined cybercrimes as criminal activities that use modern information technology, such as computer technology, network technology, etc. They further generalised the categories of cybercrimes by including illegal access (hacking), illegal interception, data interference, systems interference, misuse of devices, forgery, and electronic fraud. The South African definition of cybercrimes further expounds on their definition to include cyber extortion, unlawful acquisition, possession, provision, unlawful receipt or use of a password, access codes or similar data or devices, attempting, conspiring, aiding, abetting, inducing, inciting, instigating, instructing, commanding or procuring to commit an offence, theft of incorporeal, penalties, and competent verdicts (Department of Justice and Constitutional Development, 2016).

Cybersecurity: Cybersecurity is a computer-based discipline that deals with the presence of criminal adversaries, and as such, to deal with these adversaries, a combination of tools is needed. These might be technical tools, processes, and practices designed to protect information systems and data from attack, damage, or unauthorised access. The protection of computer systems is the sum of prevention, detection, and response (Möller, 2020).

Cyberthreats: Comprise any situation or event that carries the potential to adversely impact the operations of an organisation (including mission, functions, image, or reputation), organisational assets (digital and physical), or individuals through the use of an information system via unauthorised access, destruction, disclosure, modification of information, and denial of service. Also, it includes the potential for a threat actor to successfully exploit a particular information system's vulnerability (National Institute of Standards and Technology, 2019).

Framework: Regarding cybersecurity, a framework is a risk-based approach to dealing with and reducing cybersecurity risk within an organisation, which is achieved through the use of a set of practices, guidelines, and strategies (National Institute of Standards and Technology, 2019; Emeritus, 2022)

Information Security: The NIST defines information security as protecting information and information systems from unauthorised access, use, disclosure, disruption, modification, or destruction to assure confidentiality, integrity, and availability (National Institute of Standards and Technology, 2019)

Threat actor: A threat actor (advisory/malicious actor) is an individual or organisation that intentionally causes harm within the digital sphere. They exploit computer, network, and system weaknesses to carry out their actions (Crowdstrike, 2023).

1.4 Problem Statement

Commercial banks in South Africa have been victims of ever-increasing hacking attempts, cyber-attacks, data breaches and threats in the past few years. Clients' profiles have been illegally accessed and exposed to malicious damage (Chigada, 2020). The success of these cyber-attacks and threats can, to some extent, be credited to the ineffectiveness of the cybersecurity controls put in place by institutions or the existence of internal and external factors that might undermine the practices set in place. ISACA (2013) stated that cybersecurity is part of a complex system that continuously transforms from one stable system state to the next. An institution's cybersecurity governance, management, and assurance should be iterative, and design processes should further improve and constantly adapt to vulnerabilities, threats, and associated risks (ISACA, 2013). However, existing cybersecurity policies are not adequately deterring would-be-cybercriminals, attacks, or threats. A failure to adopt an iterative and constantly adapting approach leads to outdated governance and management policies, creating a larger attack surface whereby attackers can target institutions. The unavailability of a cybersecurity framework specifically designed for commercial banks and their complexities and localised to the country further exacerbates efforts by the banks to protect themselves and their customers. A lack of legislation and governance within the country is failing to discourage individuals from unethical behaviour (Chigada & Kyobe, 2018), thereby creating an ever more complex operating environment for banks. Thus, pertinent factors exacerbate the commission of hacking and other related malicious intentions against financial institutions' information and information systems' assets.

1.5 Research Questions

1.5.1 The Main Research Question for the Study:

- How can a cybersecurity framework mitigate cyber threats and attacks within South African commercial banks?

Furthermore, the main research question is operationalised by posing four sub-questions that seek to establish a deeper understanding of the challenges faced by commercial banks when dealing with cybersecurity and cybercrimes within South Africa. The sub-questions are listed and discussed in the next section.

1.5.2 Research Sub-questions

What factors impede commercial banks from developing a practical cybersecurity framework?

This sub-question uncovered the challenges commercial banks faced concerning developing their cybersecurity frameworks instead of adopting readily available frameworks that often were not created to solve the difficulties organisations in developing nations face today. The question assumed that frameworks developed by first-world nations often did not have to start by dealing with problems that might be considered arbitrary.

What interventions are in place to protect and mitigate the cyber threats the banks face?

This sub-question investigated the current interventions and those that commercial banks are adopting. The aim was to understand how commercial banks were responding to the ever-growing number of cyber threats that the world is currently dealing with and to know if the interventions were proving effective in protecting the digital assets of banks.

How are commercial banks affected by the cyber threats and attacks they face?

The above sub-question explored the impact cyber threats had on the operation of the banks and how the notion of ever-present threats was affecting the decision-making process regarding digital offerings from the banks. The latter part of the sub-question attempted to understand the impact of successful and unsuccessful cyber-attacks on banks' operations.

How effectively do they detect targeted attacks?

The last sub-question investigated the detection capabilities within the banks. For any institution to protect its digital estate adequately, it must first be able to detect when threat actors are carrying out attacks and, based on such detections, respond appropriately.

1.6 Research Objectives

The study aims to develop a conceptual Cybersecurity Framework for Commercial Banks in South Africa. The rise in cybersecurity threats and attacks on critical infrastructure in South Africa has become a persistent problem for organisations and stakeholders. Although multiple cybersecurity frameworks are available, a framework specifically developed for South Africa's commercial banking sector does not exist to the researcher's knowledge. Given the unique insights it would provide, a framework that considers the unique perspectives of professionals within South Africa could improve the security of critical organisations in the country. The study will achieve this by interrogating the five research objectives listed below:

1. Analysing factors that play a role in successful cyber-attacks on commercial banks in South Africa.
2. Evaluating interventions put in place to mitigate cyber threats and attacks within commercial banks.
3. Assessing the impact of cyber threats on the banks.
4. Evaluating the frequency of cyber threats within the financial sector, focusing on commercial banks.
5. Developing a conceptual Cybersecurity Framework for Commercial Banks in South Africa.

1.7 Contributions Of The Study

1.7.1 Originality/Value

In recent decades, cybersecurity has moved from a problem that seldom needed to be considered, which was often dealt with by Information Technology (IT) professionals in basements typing away frantically on their keyboards, fending off hackers, to a business problem that is now frequently discussed by executives in boardrooms. Cybersecurity has progressed from a technology risk to a business risk due to its threat to business operations (Gartner, 2021). Organisations and governments have become increasingly vulnerable to cyber threats because of how tightly integrated digital information and technology have become in day-to-day operations.

Concerning research, originality may be defined broadly as producing new findings and theories or using a novel approach, theory, method, or data (Guetzkow, Lamont & Mallard, 2004).

Based on the above definition, for this study, the researcher sought to propose a conceptual Cybersecurity Framework for Commercial Banks in South Africa, which, after reviewing numerous studies within a specific time frame and domain, he was convinced had never been attempted before in that context. Given the critical role the banking sector plays in the country, the researcher was convinced that this study would add value to the cybersecurity and banking domains in South Africa.

1.7.2 Theoretical and Methodological Contributions

The development of a conceptual cybersecurity framework brought together multiple theories that aided in pointing out the factors that have led to successful cyber-attacks in recent times and identified the trends in the types of attacks that commercial banks face. Seven factors that continually interacted with each other to produce complex and unpredictable relationships were identified. From the findings, the study proposed a theoretical confirmatory factor analysis model to validate and further highlight the correlations between the identified factors. The study also takes a unique approach to generalise its findings by collecting data from various banks in South Africa, not just from a single bank. Consequently, the study findings could be applied to the entire commercial banking sector in the country, not just one bank, and add to the existing knowledge of cybersecurity within the information systems domain.

1.7.3 Practical Contributions

The practical contributions of the study comprise recommendations that commercial banks may adopt further to improve their existing approach to cyber defence and awareness. The recommendations are based on the literature and gaps identified from the data collection phase. Commercial banks need to treat cybersecurity with the urgency that is required due to the potential impact a successful attack might have on a bank's operations and the resultant losses that might be incurred. The study identified multiple factors that contributed to the lack of cybersecurity frameworks within the commercial banking space in South Africa. It also uncovered factors that had led to successful cyber incidents that could be addressed to improve the security posture of the banks further.

This study also emphasises the need for South African banks to adopt a holistic approach that addresses people (employees and customers), processes (laws, regulations, and standards) and technology. To overcome the global phenomenon of skills shortage in security, the banks should take a proactive approach by upskilling and developing talent within their ranks instead of waiting for new talent to become available on the market. Greater emphasis must be placed on retaining existing talent and fostering employee knowledge sharing.

1.8 Scope Of The Study

This study examined the factors impeding the development of effective cybersecurity frameworks within commercial banks in South Africa, intending to develop a conceptual cybersecurity framework to address the identified factors. To achieve this, the researcher discussed previous cybersecurity incidents in the country's banking domain, the current cybersecurity legislation, and the perception of cybersecurity among employees in the banking sector. To draw a generalisation from the findings, the researcher made the utmost effort to include all the major commercial banks in the country. This also encompassed newer entrants into the banking sector who took a different approach to banking by adopting a digital-only strategy. Older banks focused more on digitising their existing offerings and establishing a better digital presence.

1.9 Research Design

1.9.1 Paradigm/Design/Methodology

The study employed a pragmatic research philosophy, which enabled it to combine multiple data collection techniques and methods to improve the reliability and validity of the research findings. Creswell and Plano Clark (2011) stated that in pragmatism, the approach taken by a researcher may combine deductive and inductive thinking as they mix both qualitative and quantitative data as they carry out the study. The methodological choice for the study was mixed methods. This was

because mixed methods made it possible to explore the qualitative aspects of the study, which were concerned with the social and human aspects of cybersecurity.
The quantitative aspect of the study was then used to verify the findings derived from the qualitative data. Creswell and Tashakkori (2007) defined mixed methods as research in which the investigator collects and analyses data, integrates the findings, and draws inferences using qualitative and quantitative approaches and techniques in a single study or programme of inquiry. Using mixed methods allows researchers to address complex research questions, find answers to exploratory and confirmatory questions within a single study, and reveal a fuller picture of the problem in practice (Greene, 2007; Teddlie & Tashakkori, 2008).

The study employed exploratory sequential mixed methods, which Creswell (2015) defined as a method wherein the researcher first begins with a qualitative research phase and explores the participants' views. The data is then analysed, and the information from the analysis is used to build a second quantitative phase. The qualitative phase may be used to create an instrument that best fits the sample under study, identify appropriate instruments for the quantitative follow-up phase, or specify variables that need to go into a follow-up quantitative study (Creswell, 2015).

For the data collection phase, semi-structured interviews were conducted using video conferencing software (Zoom and Microsoft Teams). The interviews used open-ended questions to enable the participants to give their points of view on the questions being asked. Sometimes, the participants were asked follow-up questions based on their responses. These interviews were used for qualitative data collection. For the quantitative data collection aspect of the study, surveys were distributed to potential respondents on social media platforms and through referrals for candidates deemed appropriate for the study. The survey was hosted and distributed through Google Forms.

Multivariate data analysis was then carried out on the qualitative data collected in the study. Multivariate analysis is the simultaneous analysis of relationships among several variables (Babbie, 2010). Adopting multivariate analysis made it possible to analyse the relationships between the impeding factors identified in the qualitative data. Thematic data analysis was then used to analyse the qualitative data. This method made it possible to identify and interpret patterns of meaning across the data (Clarke & Braun, 2014).

1.9.2 Research Limitations/Implications

The study encountered methodological limitations. The first limitation was data collection. With the implementation of POPIA, which limits the sharing of personal information without the express consent of the data subjects, the implications were that identified participants and respondents to the study could not share details of potential respondents and participants without first acquiring their consent. This limited the effectiveness of snowball sampling.

Secondly, although the researcher tried to obtain consent from commercial banks to conduct the study within the banks themselves, permission was not given. Furthermore, most of the survey respondents and the participants of the semi-structured interviews were employees from the big five commercial banks in South Africa, who account for about 89.4 per cent of all banking assets within the country (South African Reserve Bank Prudential Authority, 2020). Consequently, the study's findings mainly portray employees' views within the big five banks.

Additionally, newer entrants into the banking space of the country were not presented in the study. These more recent entrants are taking a digital-only approach, as opposed to traditional banks, which had to modernise their services to meet customers' demands who required more digital offerings. Regarding previous cyber incidents, the researcher could also not obtain detailed reports from the last security breaches experienced by commercial banks. The researcher had to rely on publicly available reports on media publications on previous cyber incidents in the country, which often did not give detailed information about inadequate controls that led to successful attacks.

1.10 Ethical Considerations

To adhere to strict ethical standards, an application was submitted to the University of the Western Cape's ethics department to obtain clearance to conduct the study. Furthermore, participants and respondents were required to give explicit consent to being part of the study by either verbally accepting or completing a consent form to participate in the study. The main ethical concerns for this study were the participants' and respondents' privacy and confidentiality. To address the ethical considerations, all persons taking part in the study were fully informed about the study being conducted and were made aware of the purpose of the study, of who or what group was funding the research and how the findings from the survey would be used once it was concluded.

Participants were free to withdraw at any time without any negative ramifications. Furthermore, the data collected from the participants and respondents and any resources gathered for the study were only made available to the relevant parties. Significant consideration was taken to mask the data to preserve confidentiality and anonymity if the information was distributed.

1.11 Significance Of The Research

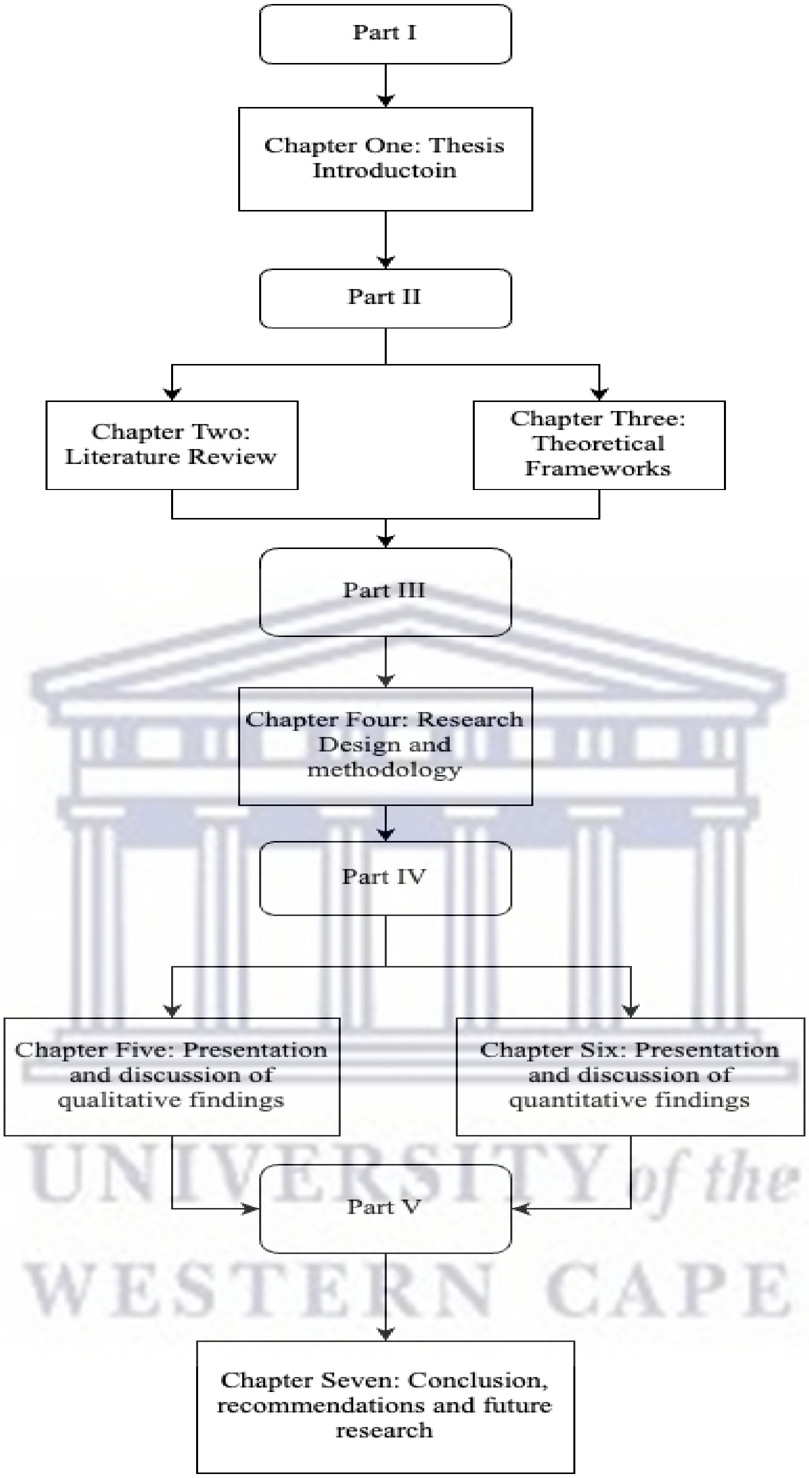
The significant contribution of this study is developing a conceptual Cybersecurity Framework for Commercial Banks in South Africa. The study also aims to create awareness among management, employees, and stakeholders about cybersecurity in South Africa and offer information, knowledge, and guidance on developing a cybersecurity culture, policies, and frameworks within commercial banks. South African commercial banks might use the proposed framework as an industry best practice framework that could then be used to support the banks.

The study would also provide more knowledge and information about the information systems discipline. It would aid researchers in understanding how commercial banks addressed cyber-attacks and threats during and after the global pandemic (COVID-19).

It also provides a foundation regarding areas that might not have been interrogated thoroughly. Hence, researchers would then be able to conduct further studies to build new knowledge within the information systems discipline.

1.12 Structure Of The Thesis

This thesis comprises five parts: Part I, Part II, Part III, PART IV, and Part V. The parts are logically arranged and serve as distinct sections of the thesis. Figure 1.1 depicts the structure of the thesis.



Part I
Chapter One: Thesis Introductoin
Part II
Chapter Two: Literature Review
Chapter Three: Theoretical Frameworks
Part III
Chapter Four: Research Design and methodology
Part IV
Chapter Five: Presentation and discussion of qualitative findings
Chapter Six: Presentation and discussion of quantitative findings
Part V
Chapter Seven: Conclusion, recommendations and future research

Figure 1.1 Thesis structure. Source (Author, 2023)

PART I

INTRODUCTION AND BACKGROUND

1.12.1 Chapter One: Introduction

This chapter provides an overview and outline of the study, which it does by introducing the research, providing background to the research problem and providing a problem statement that prompted the research. The chapter also briefly outlines the purpose of the study, the research questions, the research objectives, the research methodology adopted for the study, and the significance of the study.

PART II

LITERATURE REVIEW AND THEORETICAL FRAMEWORKS

1.12.2 Chapter Two: Literature Review

The second chapter sets out to understand the literature concerning the banking landscape in South Africa to bring context to the study. The chapter also explores the new entrants into the banking sector and the move for more digitisation in the banking space. It further explores cybersecurity, its definitions, the implications cybersecurity and cyber-attacks have had on the banking world, and the impact cyber-attacks have had on commercial banks in South Africa.

The chapter then delves into the South African government's response to cybersecurity and the laws and regulations introduced to deal with cybersecurity and build a safer South Africa. The chapter also covers common tactics, techniques, and procedures (TTPs) used by threat actors and common attacks observed in the cybersecurity domain.

1.12.3 Chapter Three: Theoretical Framework

The theoretical frameworks guiding the study are introduced and discussed in this chapter. The five theoretical frameworks comprise the National Cybersecurity Policy Framework (NCPF), Systems Theory, Chaos Theory, and Complexity Theory. The five frameworks are discussed, and their applicability to the study is demonstrated.

PART III:

RESEARCH DESIGN AND METHODOLOGY AND PRESENTATION OF FINDINGS

1.12.4 Chapter Four: Research Design and Methodology

Chapter four briefly discusses the various research designs and methodologies that were considered for the study, and it also discusses the research philosophies that underpin the study. Furthermore, it gives detailed overviews of the chosen research design, philosophy and methodology used in the study.

PART IV

1.12.5 Chapter Five: Presentation and Discussion of Qualitative Findings

Chapter five presents and discusses the qualitative findings of the study. It starts by briefly giving an overview of how the data was collected for the qualitative phase of the study. From there, it presents and discusses the participants' demographic details, such as age, gender, work experience and educational background. It then presents the thematic analysis that was carried out on the participants' responses to the interview questions posed to them.

1.12.6 Chapter Six: Presentation and Discussion of Quantitative Findings

This chapter discusses the study's quantitative findings from the survey responses. The first part of the chapter delves into the participants' demographics to understand which commercial banks were represented and the diversity of the respondents. The chapter then presents a descriptive analysis of the findings. The last part of the chapter presents the conclusions of the confirmatory factor analysis (CFA) that was carried out on the data to investigate the hypothesis that a relationship exists between the latent variables of the survey.

PART V

CONCLUSIONS, RECOMMENDATIONS, AND RESEARCH IMPLICATIONS

1.12.7 Chapter Seven: Conclusions, Recommendations, and Future Research

The concluding chapter concludes, summarises, and finalises the study by discussing the extent to which the research objectives were achieved. The findings from the survey are summarised, the study's contributions to the research domain are indicated, and possible further research is suggested. The limitations of the study are also discussed.

1.13 Chapter Summary

This chapter summarised the overall structure of the thesis; it also introduced the study by providing the background to the research, a clear and concise statement of the problem being investigated, and an overview of the study's research objectives and the research questions that guide the study. The chapter also outlined the significance of the study, concluding by giving an overview of the thesis's structure. The next section of this thesis is a literature review that provides context to the banking landscape in South Africa and explores the concept of cybersecurity and some of the most recent and noticeable cyber incidents that have occurred in recent times, globally and within the country.

PART II

LITERATURE REVIEW AND THEORETICAL FRAMEWORKS

Chapter Two : Literature Review

2.1 Introduction

This chapter seeks to examine potential responses to the research question through an extensive literature review of commercial banks in South Africa. It investigates how these banks are adopting technology to offer innovative services to their clients, to understand the competitive landscape within which South African commercial banks operate, and the unique intricacies of the banking sector in South Africa.

Secondly, it investigates the definitions of cybersecurity and the various aspects that encompass cybersecurity. Thirdly, it explores definitions of cybercrimes and the history of some of the cybercrimes perpetrated against financial institutions in South Africa. Lastly, it looks at the national legislative advancements in cybersecurity and cybercrimes in South Africa.

2.2 The South African Banking Landscape

The banking landscape in South Africa consists of the South African Reserve Bank as the central bank, five major local banks, and various smaller banks and financial institutions. This sector is considered highly developed and is ranked relatively well compared to other developed nations. In 2017, the South African banking sector ranked 11th out of 138 countries in market development in the Global Competitiveness Report. It also ranked 2nd out of 138 countries in terms of bank soundness. A robust banking system ensures the effective allocation of capital resources and the efficient management of risks, thereby preventing costly banking crises and their negative impacts on the real economy. (Schwab, 2017; Schwab, 2019). Simbanegavi *et al.* (2015) noted that the South African banking sector exhibits monopolistic competition. However, this characterisation does not imply a deficiency in efficiency or competitiveness within the market. Moyo (2018) provided further support for this view by pointing out that in 2017, the sector comprised 64 institutions, indicating a competitive environment. However, 98 per cent of the market share concentrated among the big five banks suggests monopolistic competitiveness.

With the Fourth Industrial Revolution, the South African banking sector, like other countries, has seen new entrants entering the banking market: Fintech (Financial Technology) disruptors, digital innovation start-ups and the possibility of digital currency (Central Bank Digital Currency). Banks such as Discovery Bank, TymeBank, and Bank Zero have broken the mould of what it means to be a bank in South Africa. These institutions have led the charge in a digital-first approach to banking within the country and have simultaneously posed a threat to existing banks (McKane, 2019; BusinessTech, 2021). The five big banks have also started significantly changing how they do business. Regarding digital innovation, they have had to choose between becoming part of somebody else's ecosystem or becoming a destination bank. This has led to some banks embracing a platform banking approach, which would see them offering more than financial services to their customers. Institutions such as Nedbank, First National Bank, and Standard Bank have either started this offering or intend to become platform banks (Whateley, 2021; Brink, 2020; BusinessTech, 2021).

The move to more open banking and banking as a platform could exacerbate the cybersecurity and cybercrime challenges the country already faces within the banking sector. South Africa has not been spared from becoming a target for cybercriminals. In recent years, the complexity and frequency of cyber-attacks on government, private, and critical infrastructure have increased. Multiple key government institutions have either been breached, become a target of ransomware, or had their systems disrupted through DDoS attacks (Toyana, 2021; Naidoo, 2021), while banks have either suffered from third-party breaches or had their systems breached or disrupted (Dludla, 2021).

2.3 Cybercrime In The SA Banking Industry

'Cybercrime is a socio-technical problem which is increasing at an alarming rate and will eventually replace many 'traditional' bank crimes as it transcends time and physical proximity due to its virtual nature. In addition, the convenience and anonymity of the Internet make it easy for criminals to perpetrate these crimes. These digital attacks include unauthorised access to devices, identity theft and online bank information theft. Even more concerning is its potential to infiltrate networks, resulting in mass data breaches' (South African Banking Risk Information Centre (SABRIC), n.d.).

Zhang *et al.* (2012) defined cybercrimes as criminal activities that use modern IT, such as computer technology, network technology, etc. They further generalise the categories of cybercrimes, including illegal access (hacking), illegal interception, data interference, systems interference, misuse of devices, forgery, and electronic fraud. The South African definition of cybercrimes further expounds on their definition to include cyber extortion, unlawful acquisition, possession, provision, receipt or use of a password, access codes or similar data or devices, attempting, conspiring, aiding, abetting, inducing, inciting, instigating, instructing, commanding or procuring to commit an offence, theft of incorporeal, penalties, and competent verdicts (Department of Justice and Constitutional Development, 2016). The European Crime Prevention Network (2015) identified the common types of cybercrimes as hacking, spamming, phishing, and payment fraud. That, however, is not exhaustive as traditional crimes such as fraud, bullying and child pornography, among others, are now being carried out on the Internet by perpetrators.

The number of cybercrimes has steadily increased over the past decade. A more connected world has driven this, with an increasing number of devices and users connected to the Internet and sharing personal data on devices and platforms. This has created an environment where criminals can commit crimes with varied motivations. Brar and Kumar (2018) noted that cybercrime motivations include entertainment, hacktivism, financial gain, and revenge. South Africa has also seen a scourge of cybercrimes. Critical infrastructure within the country has not been spared. In 2021, South Africa ranked seventh globally in cybersecurity exposure and had one of the highest numbers of cybercrime victims globally (Cyber Exposure Index, 2021). There are different types of cybercrimes, each carried out by perpetrators with varying motives. A typology of some of the various cybercrimes is given below:

2.3.1 Hacking

Hacking refers to actions compromising digital devices, such as computers, smartphones, tablets, networks, and information systems, through unauthorised access to any account or computer system. The intention is to misuse devices such as computers, smartphones, tablets, and networks to cause damage or corrupt information systems, gather information on victims, steal data or disrupt access to a service (Fortinet, 2021; Malwarebytes, 2021). When it comes to hacking, there are different types of hackers; criminal hackers are called black hat hackers. Professional security expert hackers are called white hat hackers, and grey hat hackers sit somewhere between black and white hat hackers. Black hat hackers are criminal hackers who go out of their way to discover and exploit computer systems and software vulnerabilities for financial gain or malicious purposes. White hat hackers strive to improve the security of computer systems and software by finding vulnerabilities within organisational computer systems and software. Grey hat hackers are those who unlawfully break into computer systems and networks but report their exploits to organisations to gain a small fee (bounty) and help organisations repair the vulnerabilities in their systems (Fortinet, 2021; Malwarebytes, 2021; Ezeji, Olutola & Bello, 2018).

2.3.2 Identity Fraud

Identity fraud is when a perpetrator uses one’s personally identifiable information to pretend to be a victim to commit fraud or to gain other financial benefits. The perpetrator usually gains the victim's information through various means such as phishing, card, automatic teller machine (ATM) skimming, wi-fi hacking or traditional means such as dumpster diving through the victim’s mail (van der Kleut, 2021). The stolen identities might also be sold to terrorists or common criminals who use the identities to avoid authorities or circumvent immigration laws.

The victims of these cybercrimes are usually chosen for convenience (Ezeji *et al.*, 2018). SABRIC (2023) stated that identity theft occurs when criminals assume a victim's identity and acquire retail or banking accounts by using the assumed identity. Chigada (2020) highlighted a worrisome trend that had seen an increase in identity theft and fraud that had led to substantial financial losses by victims of economic crime.

2.3.3 Cyber-terrorism

A universally accepted definition of cyber-terrorism does not exist. However, Plotnek and Slay (2021) opined that cyber-terrorism might be defined as “the deliberate attack or threat thereof by non-state actors with the intent to use cyberspace to cause real-world consequences to induce fear or coerce civilians, government, or non-government targets; in pursuit of social or ideological objectives.

Real-world consequences outside cyberspace include physical, psychosocial, political, economic, ecological, or otherwise." Mothibi and Amali (2018) suggested that cyber-terrorism begins when a clandestine or informal group uses cyberspace to go against societal norms and values to impose their beliefs and ideologies on others.

2.3.4 Cyberwarfare

Cyberwarfare is a nation-state's actions to penetrate another nation's computers or networks to cause damage or disruption. These attacks may be aimed at critical infrastructure within a nation (Ezeji *et al.*, 2018). Taddeo (2012) defined cyber warfare as using ICTs within an offensive or defensive military strategy endorsed by a state to disrupt or control a target's resources. These actions are carried out in cyberspace with agents and targeted action that ranges from physical to non-physical action.

2.3.5 Cyberstalking

This is a crime that may be described as online harassment. It is an electronic extension of talking, which involves a terrifying pursuit of the victim and usually involves following an individual's movements across the Internet (Mothibi & Amali, 2018). Chang (2020) postulated that cyberstalking falls under the larger umbrella of digital harassment, which refers to harmful interpersonal behaviours experienced by individuals through digital platforms, mobile devices, or other electronic communication devices.

The perpetrators of these crimes usually take advantage of features of digital technology such as low cost, ease of use, and the ability to remain anonymous. The key difference between cyberstalking and traditional stalking is that cyberstalking is not restricted to geographical location. The offenders could be geographically far from the victims, and cyberstalking can involve third parties on the Internet.

2.3.6 Revenge Pornography

Bloom (2016) defines revenge porn as non-consensual pornography/involuntary pornography, which involves the distribution of sexually graphic content by an individual where at least one of the individuals involved did not consent to the dissemination of the content. Musoni (2019) states that the harm caused by revenge porn is not trivial.

The crime often raises the risk of physical attacks as the perpetrators usually share full names, addresses, and telephone numbers with the graphic content of their victims. Within South Africa, revenge porn became a criminal act after the Films and Publications Amendment Bill was signed into law in July 2020.

2.4 COVID-19 And Cybercrimes

COVID-19 is an infectious disease caused by the SARS-CoV-2 virus; it is part of the coronavirus family that causes various diseases ranging from head or chest colds to more severe conditions like acute respiratory syndrome. The virus was first identified amid an outbreak of respiratory illness cases in Wuhan, China (Centre for Disease Control and Prevention, 2021; World Health Organization, 2020). The World Health Organisation (WHO) declared the virus a pandemic in March 2020. Since then, the virus has spread across the entire globe and has significantly disrupted life (World Health Organization, 2020). The pandemic spread globally and affected how businesses operated and defined a new normal: working from home, a lack of social interaction and low levels of physical activity.

The spread of the global pandemic did not deter cybercriminals. They seized the opportunity presented by the pandemic to carry out various crimes. The World Economic Forum reported that cybercriminals exploited the pandemic by taking advantage of the demand for information on the virus, spreading confusion about the virus, spreading fear, and exploiting the boredom brought about by confinement to find new ways of delivering malware, ransomware, and phishing (World Economic Forum, 2020). A report issued by Interpol stated that cybercriminals adapted to COVID-19 and started to launch COVID-19 targeted attacks. There was an increase in malicious domains with the words 'COVID' or 'Corona,' and numerous fake websites related to COVID-19 were created. There was an increase in the exploitation of the vulnerabilities of systems, networks and applications used by businesses, governments, and schools to support staff who were now working remotely (INTERPOL, 2020). The new work-from-home normal introduced by COVID-19 increased the number of cyber risks staff from organisations faced. Because individuals connected to organisational networks through less secure and unreliable Internet connections and staff were working from remote locations, unauthorised individuals could quickly obtain and abuse their connected and authenticated devices (Chigada & Madzinga, 2021). Figure 2.1 depicts the increase in COVID-19-related cyber-attacks from December 2019, when the virus was first identified, to

April 2020. During that time and in the following months, cybercriminals launched three primary phishing attacks: scamming, brand impersonation, and compromising business emails. A business email compromise is a scam whereby criminals send an email message that appears to come from a known and valid source, making a legitimate request with the most common objective being to convince the target to send money to the criminal (Check Point Software Technologies Ltd, n.d.; Federal Bureau of Investigation, 2020; Minnaar, 2020).

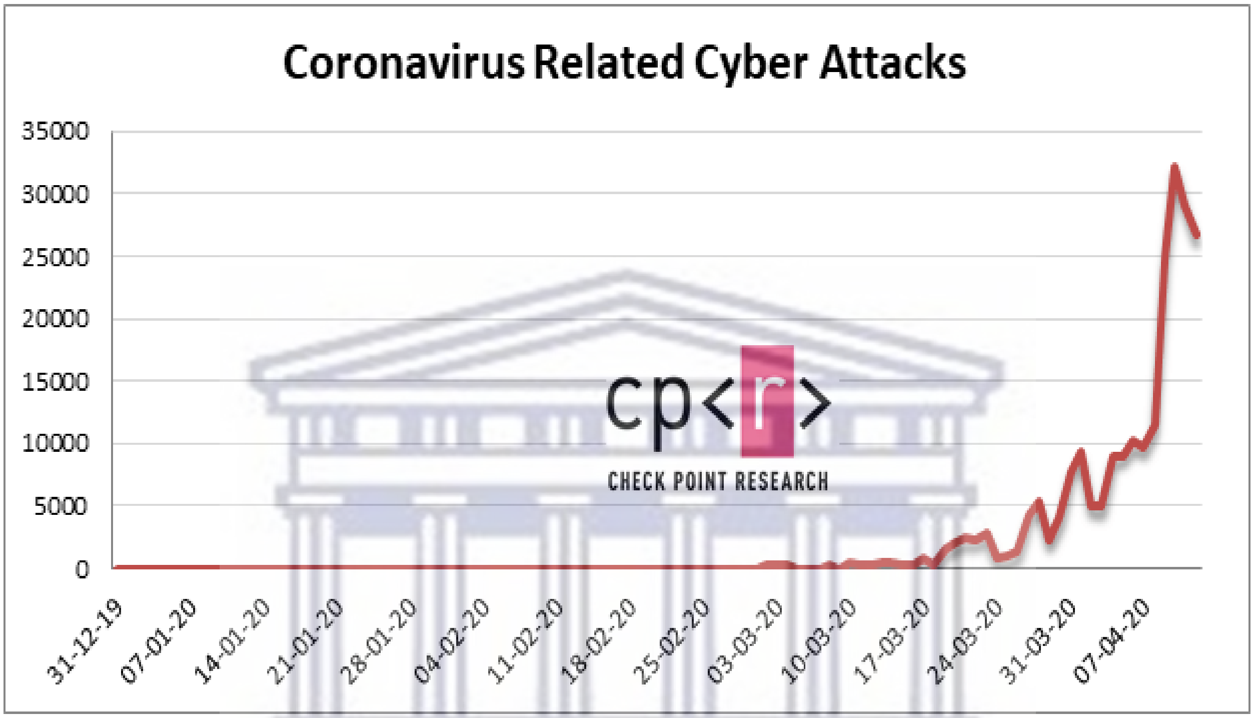


Figure 2.1 Detected Coronavirus Related Cyber-Attacks. Source (Check Point Software Technologies Ltd, 2020)

2.4.1 Cyber-attacks

Gaumer, Mortier and Moutaib (2016) stated that cybercrimes were among the most significant issues for financial and banking institutions. This is because, recently, hackers started to shift towards a strategy to target financial institutions instead of end-users. For these attacks to be successful, they had to evade the cyber kill chain effectively. The kill chain is a framework developed by Lockheed Martin that outlines seven phases of an attack. These phases are reconnaissance, weaponisation, delivery, exploitation, installation, command and control (C2), and actions on objectives. Figure 2.2 details the seven phases.

An example of such a shift towards targeting financial institutions is evident in the Carbanak campaign (Kaspersky Lab, 2015), discovered by Kaspersky Lab and deemed one of the most significant cyber-attacks ever. The campaign used APTs[1] to gain footholds in targeted organisations and execute their exploits through well-known vulnerabilities such as CVE-2012-0158[2] and CVE-2013-3906[3], which target tools and software employees use regularly. Marchetti, Colajanni, Messori, Aniello, and Vigfusson (2012) discussed how the number of cyber-attacks on critical financial infrastructure has increased as modern society has become more reliant on networked systems.

Attacks were mainly distributed and carried out by multiple players, usually targeting various aspects related to financial institutions. Marchetti *et al.* (2012) outlined five recent common distributed attacks performed on financial institutions. These attacks are Man-in-the-Middle (MitM), Distributed Portscan, DDoS, Session hijacking, and Malware-Based Attacks. Cater (2017), through the SWIFT Institute, also reported on the increasing number of attacks on external bank services that financial institutions use to facilitate their transactions. An attack on the SWIFT network is an example of indirect cyber-attacks on financial institutions.

In a report published by IBM (2017), the company detailed how most cyber-attacks in 2016 were aimed at financial services. A substantial portion of these attacks originated internally within organisations. This suggests that threats faced by financial institutions are both external and internal. The frequency and scale of cyber-attacks in South Africa have also been increasing. Van Niekerk (2017) highlighted the major cyber incidents in South Africa from 1994 until 2016.

His findings showed that there has been an upward trend in the number of incidents the country has faced over the years, in line with the global trend. South Africa went from having only two major cybersecurity incidents in 1994 to having approximately twelve significant incidents in 2016. He also stated that the number of threat actors that have targeted South African systems has increased over the years. These actors include APTs, hacktivists, nation-states, criminal organisations, and internal threats. These threat actors have different motivations.

[1] APT: advanced persistent threat (a network attack in which an unauthorised person gains access to a network and stays hidden and undetected for an extended period, monitoring the network and stealing data

[2] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0158

[3] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3906

Figure 2.3 depicts different threat actors and their typical motivations. The complexities and types of attacks have also increased over the years, from data exposure and denial of service attacks to ransomware attacks.

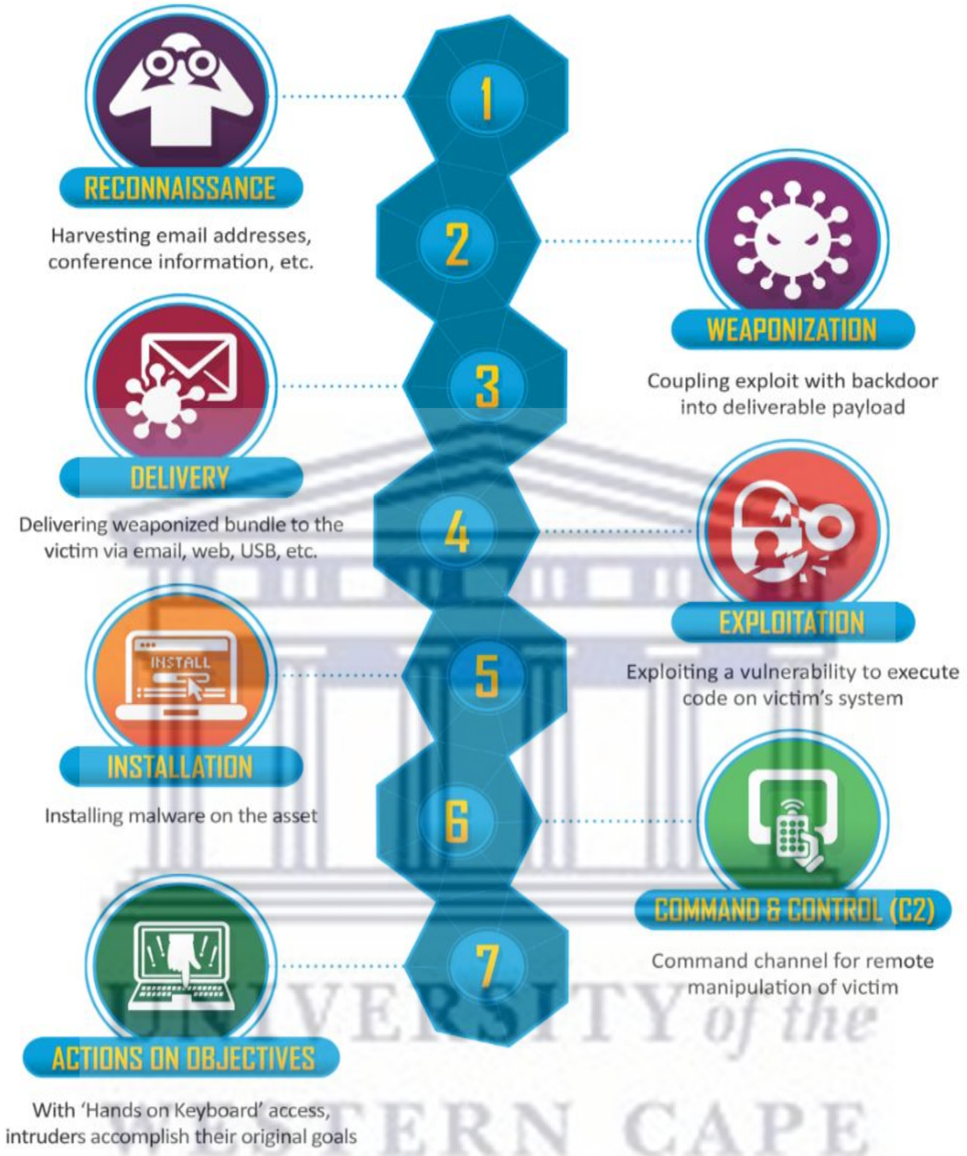

1
RECONNAISSANCE
Harvesting email addresses, conference information, etc.
2
WEAPONIZATION
Coupling exploit with backdoor into deliverable payload
3
DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc.
4
EXPLOITATION
Exploiting a vulnerability to execute code on victim's system
5
INSTALL
INSTALLATION
Installing malware on the asset
6
COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim
7
ACTIONS ON OBJECTIVES
With 'Hands on Keyboard' access, intruders accomplish their original goals

Figure 2.2 Lockheed Martin Cyber Kill Chain. Source (Lockheed Martin Corporation, 2011)

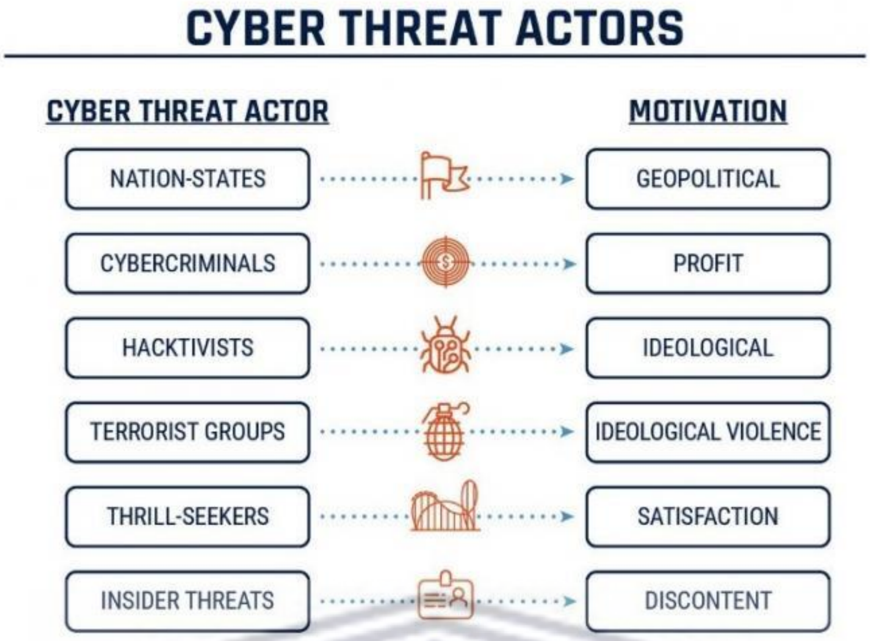
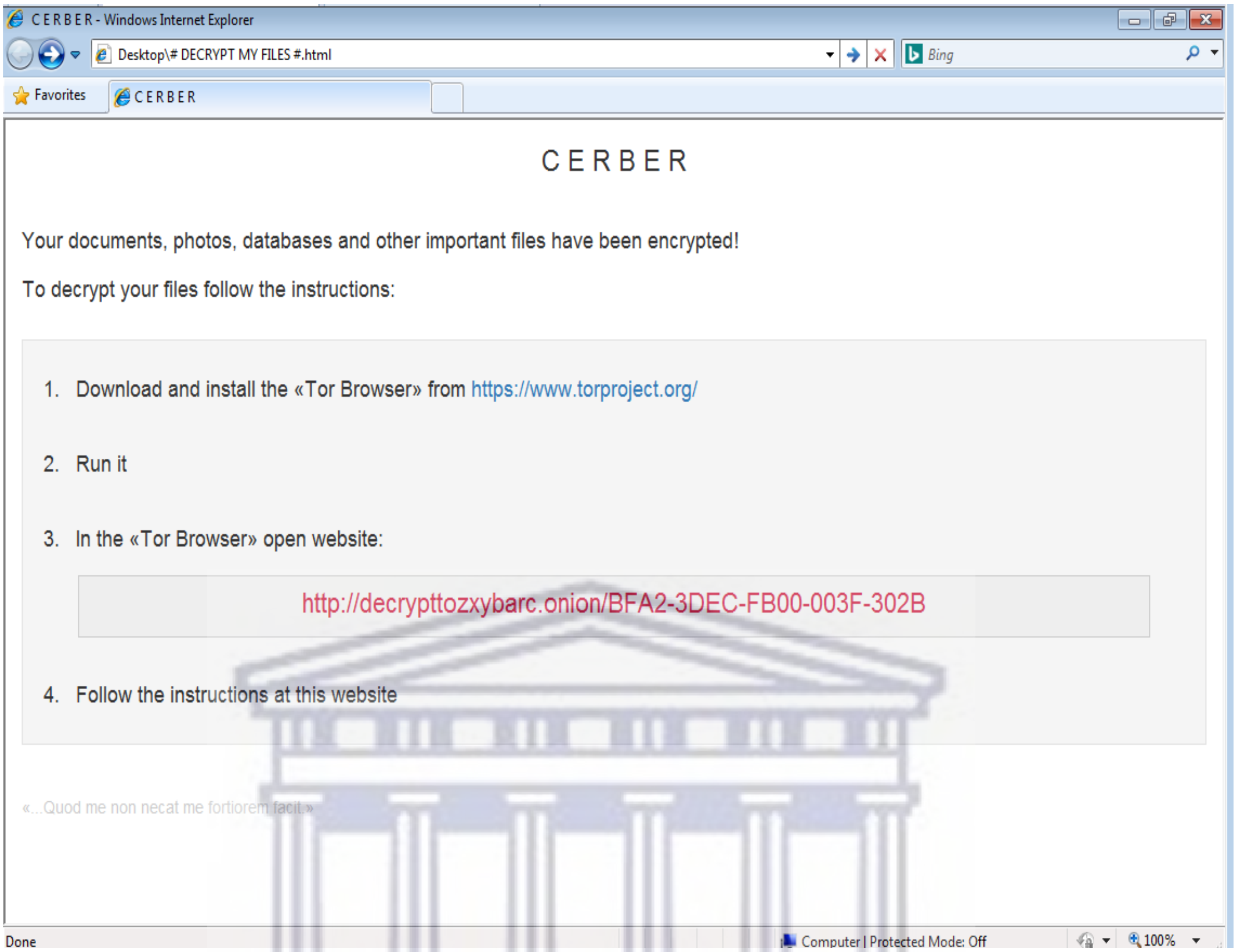


Figure 2.3 Cyber Threat Actors. Source (Northern Ireland Cyber Security Centre, 2023)

2.4.2 Common Cyber-attacks

Zero-day exploit: These attacks use unknown or undisclosed hardware and software vulnerabilities. The vulnerabilities are usually discovered internally by the organisations producing the hardware or software, by external security researchers or by cyber-attackers who exploit them until the organisations discover them (IBM, n.d.; Check Point Software Technologies Ltd, n.d.).

Ransomware: This is advanced malware that leverages weaknesses in systems to move within an organisation's infrastructure and encrypt files using strong encryption to hold data or the encrypted system hostage in exchange for a ransom; it is either delivered onto the victim's computer through a download from a website or within an email attachment (Fortinet, n.d.). Its complexity lies in that some ransomware can evade traditional antivirus software. According to an IBM report, Ransomware accounted for 23 per cent of all cyber-attacks in 2020. An Interpol report showed that South Africa had the second-highest number of ransomware detections in Africa in 2020 (IBM, n.d.; INTERPOL, 2021). Figure 2.4 depicts an example of a ransomware demand from an attacker; these notes usually provide payment information and a threat of what happens if the victim does not pay the ransom (Trend Micro, 2016).


CERBER - Windows Internet Explorer
Desktop\# DECRYPT MY FILES #.html
Bing
Favorites
CERBER
Done
Computer | Protected Mode: Off
100%

CERBER

Your documents, photos, databases and other important files have been encrypted!

To decrypt your files follow the instructions:

1. Download and install the «Tor Browser» from https://www.torproject.org/
2. Run it
3. In the «Tor Browser» open website:

   http://decrypttozxybarc.onion/BFA2-3DEC-FB00-003F-302B

4. Follow the instructions at this website

«...Quod me non necat me fortiorem facit.»

Figure 2.4 Cerber Ransom Note Source: (Trend Micro, 2016)

Phishing: Phishing is a type of cyber-attack that employs email, SMS, phone, social media, or social engineering techniques to get victims to share sensitive information such as passwords and account numbers or download malicious software. This is done by sending fraudulent communications that appear to originate from a reputable source (Cisco, n.d.; Crowd Strike, 2021).

Man-in-the-Middle (MitM) attack: This is a form of active wiretapping attack in which the attack intercepts, modifies, and monitors communicated data between hosts masquerading as one or more entities involved in the communication (National Institute of Standards and Technology, n.d.). To carry out this attack, attackers position themselves between communicating parties and break the communication connection into two pieces. They create a separate encrypted connection between the client and the server (Check Point Software Technologies Ltd, n.d.). Figure 2.5 depicts how a MitM attack works.

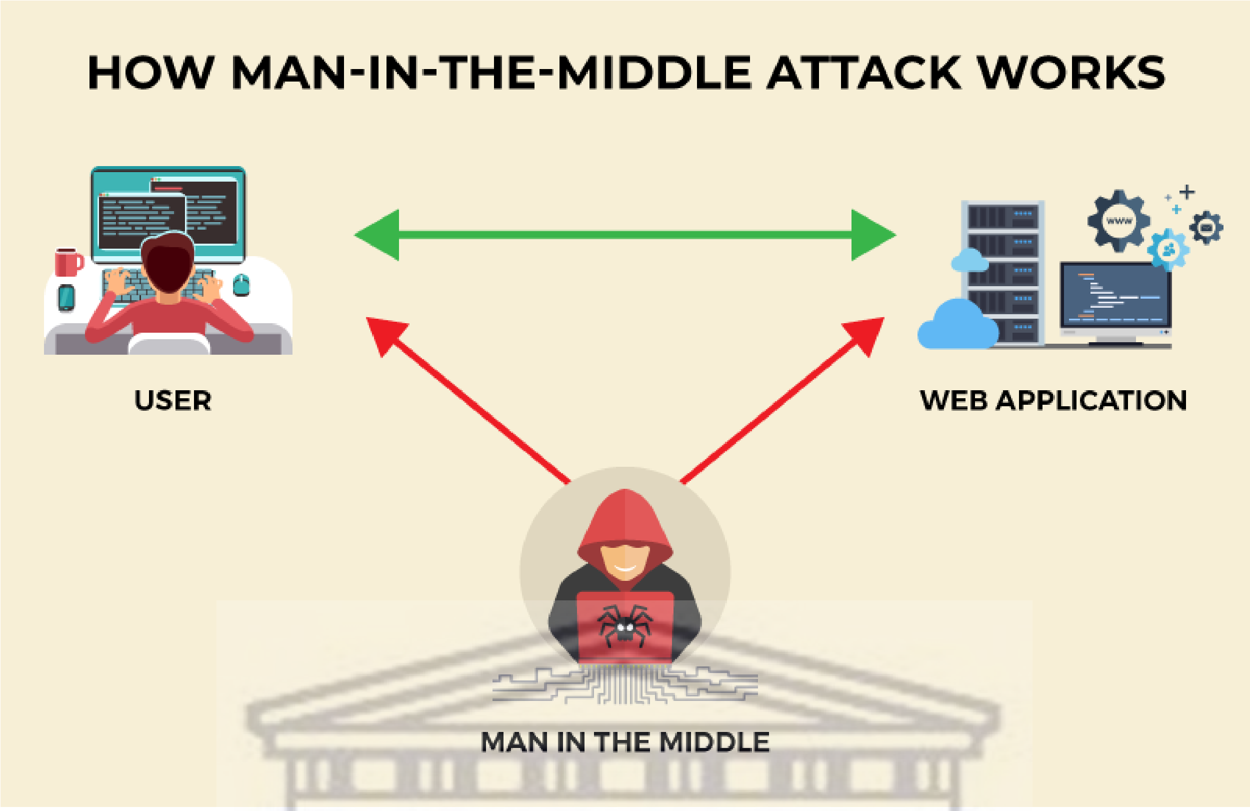


Figure 2.5 How Man-in-the-Middle Attack Works Source: (CISO Mag, 2021)

Distributed Portscan: this attack aims to find TCP/UDP ports that have unintentionally been left open by the institution. Given the right circumstances, attackers can gain a foothold in the institution's internal network through these open service ports. This attack also serves as a reconnaissance attack to understand the various services the institutions have exposed on their external network.

Distributed Denial of Service Attacks (DDoS): this attack aims to prevent the IT infrastructure of the targeted institution from delivering expected services. Multiple botnets usually carry out this attack against specific services in an institution.

Session hijacking: These attacks involve using valid session IDs, usually in cookies. These session IDs are retrieved using other exploits, such as cross-site scripting (XSS). Once the exploit is successful, attackers can use the valid session IDs to continue transacting as legitimate users.

Malware-Based Attacks: Internet worms and Trojans represent well-known threats to the security of networked information systems. These attacks usually involve specially crafted malware that uses existing system vulnerabilities to gain a foothold and execute malicious payloads.

2.4.3 Noticeable Cyber-attacks In South Africa

As mentioned by van Niekerk (2017) and the SABRIC, the number of cybercrimes reported in South Africa has seen a sharp increase over the past few decades, with 2019 seeing a 20 per cent increase in the number of digital banking incidents within South Africa (South African Banking Risk Information Centre (SABRIC), 2019). This subsection will highlight some of the significant cybercrimes related to commercial banks in South Africa that have taken place in recent history. The incidents will be presented in chronological order.

Van Niekerk (2017) stated that the first cybercrime incident against a commercial bank in South Africa occurred in 2003 when Absa Bank lost approximately ZAR 500,000 due to a hack. In this case, the threat actor compromised the users by sending an email containing a trojan which obtained the banking details and PINs of the victims when opened. The hackers then used the victims' computers to access their bank accounts, bypassing security controls and making it seem like a legitimate session. They then withdrew money from the victims' accounts (IOL Media, 2003). Threat actors used social engineering to obtain identity documents in a separate incident. They then proceeded to open a parallel Internet banking account with the authority to transfer funds from the victim’s account to other accounts. This incident did not compromise the victim’s identification number (PIN) (Vecchiatto, 2003).

In 2006, in three months, account user details for clients from three commercial banks in South Africa were compromised. The compromised credentials were then used to transfer money from the victim’s accounts into either cell phones or Telkom prepaid accounts (IOL Media, 2006). The threat actor, in this case, found a way to hack into either business accounts or personal accounts belonging to the victims, using malicious tools such as spyware, backdoor trojans and keyloggers; this breach cost an estimated USD 80,000 (Oiaga, 2006).

An attack possibly aided by Landbank and Absa Bank employees occurred in December 2010. A syndicate hacked into the Landbank’s infrastructure and obtained secret passwords only select personnel could access. The syndicate then proceeded to set up automated fund transfers to multiple companies. However, the attackers were unsuccessful, as bankers at Absa noticed the suspicious transactions and froze the accounts (Potgieter, 2011).

Postbank suffered a loss of ZAR 42 million over three days. A syndicate managed to infiltrate the bank's infrastructure through an employee's computer connected to the bank's server. They then used the compromised credentials of two low-level employees to increase account withdrawal limits. With this in hand, the syndicate sent money to accounts and withdrew the funds over three days at multiple ATMs across South Africa (Swart & Wa Afrika, 2012).

Standard Bank South Africa suffered a massive cyber-attack in 2016, leading to the bank losing ZAR 300 million through an ATM fraud attack in Japan. In the coordinated attack, about one hundred people used forged Standard Bank credit cards to withdraw money from 1400 ATMs throughout Japan (Moyo, 2016). It was suspected that hackers broke into the bank's digital infrastructure and obtained about 3000 sets of personal data that were subsequently used in the attack (News24Wire, 2016).

In 2019, South African banks were hit by a massive DDoS targeting multiple banks nationwide. The attack was ransom-driven, with the threat actors sending ransom notes to employee email addresses and unattended email addresses within the targeted banks (Fin24, 2019). This attack disrupted online and mobile app banking (McKane, 2019).

Absa South Africa was a victim of an insider attacker after an employee illegally accessed and shared customer information with third parties. The data accessed by the employee contained a mix of sensitive and marketing information (Thompson & Farber, 2020). In the same year, Nedbank suffered a data breach through one of its third-party service providers (Computer Facilities (Pty) Ltd). The compromise involved the leaking of personally identifiable information of some Nedbank clients. The third-party breach affected approximately 1.7 million clients, with 1.1 million active clients (Nedbank, 2020).

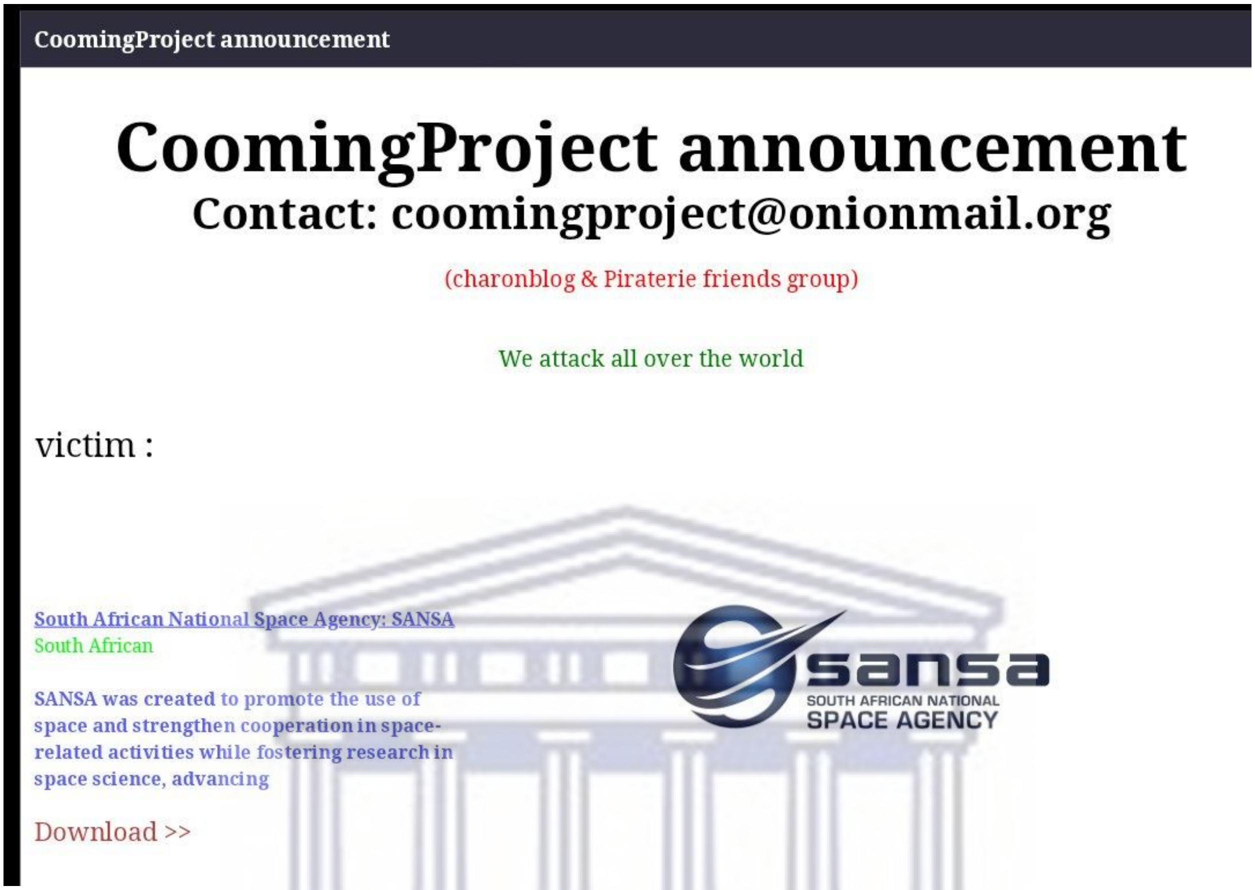
The Department of Justice in South Africa had its information systems encrypted and rendered unavailable due to ransomware. The breach happened on 6 September 2021, leading to collapsed court systems across the country. It is alleged that the criminals demanded a ransom of ZAR 33 million. The same day the Department of Justice was hacked, the South African National Space Agency also had some of its systems encrypted and held for ransom (Toyana, 2021; Illidge, 2021). Figure 2.6 depicts an announcement by the criminals (coomingProject gang) who hacked the South African National Space Agency.

The University of Mpumalanga was a victim of a business email compromise. A criminal forged an email to convince a staff member that the details of the asset manager the university used had changed. The staff member subsequently sent ZAR 100 million to the new bank account provided in the forged email (MyBroadBand, 2021). Transnet, a South African rail, port, and pipeline company, declared force majeure on its ports division after a cyber-attack left it unable to digitally track and account for thousands of containers at the country's ports. This attack forced the company to operate manually, thus delaying long shipping containers. This was one of the most significant attacks on maritime infrastructure within South Africa and was part of a global trend that has seen a 400 per cent increase in maritime cyber hacks (Booth, 2021; Reva, 2021).

As a response and acknowledgement of the ever-increasing cyber threat, in 2005, the South African Police Service (SAPS) and the Council for Scientific and Industrial Research (CSIR) embarked on a project codenamed 'Charlie' from the project recommendations that were put forth for the development of a national Computer Security Incident Response Teams (CSIRT). The government's failure to develop a national CSIRT led to establishing the banking sector CSIRT under the SABRIC banner (South African Banking Risk Information Centre (SABRIC), n.d.). In 2015, the SABRIC CSIRT became operational and set out to align its activities with the NCPF and to achieve the objectives shown below as a response to cyber threats:

- Develop and mandate sector-wide strategies to improve cyber resilience.
- Develop local capabilities to monitor the threat landscape.
- Serve as a conduit for banking sector partners to facilitate knowledge sharing on cybercriminals.
- Explore proactive measures to detect, deter, and defend against cyber threats.

In the years following the establishment of the SABRIC CSIRT, SABRIC has served as an independent authority providing insights into the banking threat landscape of South Africa and disseminating information and resources to the public and financial institutions against cyber threats and attacks.



CoomingProject announcement

CoomingProject announcement
Contact: coomingproject@onionmail.org

(charonblog & Piraterie friends group)

We attack all over the world

victim :

South African National Space Agency: SANSA
South African

SANSA was created to promote the use of space and strengthen cooperation in space-related activities while fostering research in space science, advancing

Download >>

Figure 2.6 CoomingProject gang announcement. Source: (Vermeulen, 2021)

2.4.4 Effects Of Cybercrime On Banks/Economy

The losses incurred by financial institutions at the hands of cyber-attacks and breaches have increased recently. In the Carbanak campaign, financial institutions lost nearly US$ 1 billion (Kaspersky Lab, 2015). The losses experienced by financial institutions go further than monetary losses. Financial institutions usually suffer irreparable damage through reputational damage and loss of investor confidence. A report published by Accenture and Ponemon Institute LLC (2019) showed that the costs of all types of cyber-attacks are increasing annually, with the average price of an attack totalling US$ 13.0 million in 2018.

Mossburg, Gelinne and Calzada (2016) supported the sentiment that financial losses were not the only costs associated with a cyber breach. Furthermore, they reported that institutions can suffer from loss of intellectual property, devaluation of a trade name, and impact of operational disruption or destruction. Smith and Lostri (2020) stated that other hidden costs associated with cyber-attacks are opportunity cost, which is income lost when a resource cannot be used or when a service cannot be provided; incident response costs, which means the average time it takes an organisation to move from discovery of a cyber incident to its remediation, and cyber risk insurance. Hunton (2012) further postulated that data had become the new digital currency of cybercrimes, adding to the overall cost of cyber breaches. Data might not have tangible monetary value, but losing a client's personally identifiable information can affect an institution badly. All these factors further increase an institution's recovery time when they realise they have been cyber-attack targets.

For publicly traded companies, the announcement of cybercrime often negatively impacts the market value of their stock prices. This negative impact is sometimes not permanent. However, the affected company still incurs market losses (Smith, Jones, Johnson, & Smith, 2019). Publicly traded companies, retail stores, healthcare facilities, and providers tend to be targets of cybercrime because of the vast amount of transactional and healthcare records they hold and the numerous amounts of personal information that criminals can retrieve. When such companies suffer cyber-attacks and their client's personal information is lost to criminals, clients tend to lose faith in the company because the attack creates a sense of fear around the security of their personal information and transaction information. The cost of this on a larger scale damages the economic growth prospects of the companies affects trade and hampers the company's ability to be competitive and innovative.

Ratten (2019) postulated that cybercrime has also affected how organisations share information to drive innovation and competitiveness. The amount of information companies share now needs to be carefully considered, and policies must be implemented to deal with the possibility of cybercrime. Innovation must be carefully managed with entities that companies trust to ensure that confidential and sensitive information is not used maliciously.

2.5 Cybersecurity

The terms cybersecurity and information security are often used interchangeably. Although these terms share various similarities, using them interchangeably takes away from the meaning and significance of each. Chigada and Kyobe (2018) posited that cybersecurity entails a multidisciplinary approach of up legal, regulatory, technical and non-technical mechanisms, intending to mitigate, combat, minimise and protect against cyber-attacks and threats. The International Telecommunications Union [ITU] (2017) 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. Organisation and users' assets include connected computing devices, personnel, infrastructure, applications, services, telecommunication systems, and the totality of transmitted and stored information in the cyber environment (The International Telecommunications Union, 2017).

Kabanda (2018) defined cybersecurity as "protecting Internet-connected systems, including hardware, software, and data, from cyber-attacks". Xulu (2022) posited that cybersecurity is the organisation and collection of resources, processes, and structures (policies and standards) to protect cyberspace and Internet-enabled systems from malicious actors. The NIST defines information security as protecting information and information systems from unauthorised access, use, disclosure, disruption, modification, or destruction to provide confidentiality, integrity, and availability (National Institute of Standards and Technology, 2019).

Von Solms and van Niekerk (2013) stated that information security protects information as an asset from possible harm from various threats and vulnerabilities. They posited that cybersecurity is not necessarily the protection of cyberspace but also the protection of those systems that function in cyberspace and any of their assets that can be reached via cyberspace. This can be observed in their definition of cybersecurity, which postulates that cybersecurity is the fact that all assets should be protected and need to be protected due to the vulnerabilities that exist due to the use of ICT (Van Solms & van Niekerk, 2013). These assets include connected computing devices, personnel, infrastructure, applications, services, those that function in cyberspace, and all transmitted or stored information in the cyber environment. From these definitions, it is evident that cybersecurity has moved from being about technical aspects of IT to a more holistic approach. To support this, Von Solms and van Niekerk (2013) and Möller (2020) posited that there are six elements of cybersecurity, namely;

- Application Security – security measures at the application level to make applications more secure by finding and remediating vulnerabilities.

- Computer Security protects computer systems or networks from harm, hijacking, unauthorised access, or service disruption.
- Data Security –a set of standards and technologies, such as data loss prevention (DLPs), to prevent unauthorised access to information systems and databases.
- Disaster Recovery and Business Continuity Planning – comprises practices to limit the impact of cyber threats and attacks to get organisations functional as quickly as possible after unexpected security incidents.
- Information Security – this element includes a set of strategies designed to maintain the CIA Triad of confidentiality, integrity, and availability of the application, data, and any other information systems an organisation might have.
- Network Security – many technologies, devices, and processes to secure networks within organisations, including configuring rules to maintain CIA.

2.5.1 Cybersecurity Challenges

Over time, the increasing complexity, frequency, and severity of cyber-attacks targeting financial institutions bring forth the inevitability and the impossibility of ultimately protecting the integrity of critical computer systems and data (Dupont, 2019). Being completely secure is impossible given the multiple challenges within cybersecurity, an ever-changing, fast-paced environment of technology and threat actor tools. The Fourth Industrial Revolution also adds complexity, representing a fundamental change in how humans live and work. It enables the merger of the physical, digital, and biological worlds, the combination of cyber-physical systems, the Internet of Things and the Internet of Systems, smart factories and fusing technologies in ways that create promise and peril (Schwab, 2015; Marr, 2018).

The European Union Agency for Cybersecurity (ENISA) (2021) identifies some of the challenges in cybersecurity as a lack of sufficient information security expertise and awareness, incomplete organisational policies, a reluctance to fund security, a lack of accountability, fragmentation of security technical standards, supply chain management complexity, interoperability of devices, platforms and frameworks, and a lack of technical capabilities (Malatras, Skouloudi, & Koukounas, 2019). Blum (2020) added to the list of challenges by identifying ineffective communication, hard-to-change culture and the lack of solid leadership within organisations.

Strong leadership would like to see cybersecurity move out from operating in a silo to a more cross-functional operation that would give cybersecurity leaders the resources and support structures that are required to defend the organisations they serve adequately.

Furthermore, motivating, retaining, and hiring key cybersecurity staff was highlighted as challenging for organisations amid the threat of human error or misconduct. Ahmed, Sharif, Kabir and Al-Maimani (2012) attributed most cyber-attacks to human error and the abandonment of security policies that mitigated cyber threats and attacks. Wells, Camelio, Williams, and White (2014) further posited how a lack of awareness when creating systems can introduce security vulnerabilities. Marble, Lawless, Mittu, Coyne, Abramson and Sibley (2015) discussed how the human element is the common thread among all cyber threats. The authors shared how using malicious software, hackers could exploit the motives of users who simply seek to achieve their goals. Gaumer *et al*. (2016) detailed how hackers have become skilled in the technical aspects of cybersecurity and in exploiting human frailties. Hackers no longer hesitate to interact with their human targets through phishing, vishing or, in extreme cases, through real meetings to build trust and manipulate their victims' behaviour.

The SOC comprises CSIRT and other functions that form an effective cybersecurity architecture within any institution. The security operations centre and the CSIRT are responsible for dealing with cybersecurity incidents that occur within institutions. They do this by investigating, triaging, responding to, and remediating incidents (CompTIA, 2021; Cybersecurity & Infrastructure Security Agency, 2007). They form the core of any cybersecurity undertaking within an institution. Catota *et al.* (2018) (Table 2.1) listed some barriers and contributing factors to CSIRT challenges. These factors and barriers are remarkably like those mentioned by other authors, corroborating the common theme of challenges faced in cybersecurity.

Like other African countries and developed nations, South Africa has faced its share of cybersecurity challenges. There has been an increase in the number of cyber-attacks and cyber-victimisation in Africa, as cybercriminals see Africa as a haven where they can operate illegally (Kshetri, 2019). This is because cybersecurity is considered a luxury in some African economies. There is also an apparent lack of skills, with an estimated shortage of about 100,000 cybersecurity personnel by 2020 (Kshetri, 2019). According to Accenture (2020), South Africa had the third most cybercrime victims worldwide, ranking it as one of the most targeted nations globally. South Africa is an attractive target to threat actors because they view South African organisations as having lower defence barriers than their more developed counterparts. Furthermore, Winjit (2021) stated that what made South Africa attractive to such criminals was the presence of weak cybercrime laws, which reduced the chances of detection and prosecution, a lack of investment in cybersecurity and poor public knowledge of cybersecurity within the country. Ramluckan, van Niekerk, and Leenen (2020) first attributed some of the challenges South Africa faces regarding cybersecurity to a rigid National Qualifications (NQF) structure that made it difficult for students to undertake multidisciplinary studies, which are often required with cybersecurity, due to its diverse nature. Secondly, they posited that the South African schooling system does not provide an adequate grounding in Science, Technology, Engineering, and Mathematics (STEM), a prerequisite for those seeking a future in cybersecurity. Lastly, the lack of core researchers and no evidence of young emerging researchers within South Africa poses a challenge to the future of cybersecurity within the country.

Table 2.1 Barriers and Factors Affecting CSIRT Adapted from Catota, Morgan, & Sicker (2018)

	Barriers	Contributory factors
People	• Lack of awareness • Insufficient human resources • Insufficient professionals in the market • Employee turnover	• Insufficient budget • Institutional business profile • Insufficient academic education in cybersecurity • Lack of knowledge
Technology	• Lack of technology • Technology implementation and updating	• Insufficient budget • Diversity of systems and legacy systems
Process	• Internal coordination/communication	• Business priorities • Lack of empowerment

	• Effectiveness of security controls • Visibility of the network(detection) • Lack of training	• Operational daily activities • Insufficient budget
Externalities	• Lack of collaboration/sharing • Coordination with financial institutions • External support of Internet providers • Lack of local specialised personnel • Inappropriate legal framework	• Lack of international cooperation • Lack of communicative procedures • Lack of trust

2.5.2 Cybersecurity Policies

Karlsson, Hedström and Goldkuhl (2017) defined information security policy as a 'direction-giving document' (Hone and Eloff, 2002, cited in Karlsson *et al.*, 2017) for defining acceptable behaviour for employees when using an organisation's information assets (Davis & Olson, 1985, in Karlsson, *et al.*, 2017). The information security policy outlines employees' behaviour when dealing with an organisation's information systems.

Failure to adhere to the guidelines in the security policy often leads to employees weakening the organisation's security posture. Mbelli and Dwolatzky (2016) identified poor or no policy and standard management as threats to cyberbanking in South Africa. This notion is further supported by Li, He, Xu, Ash, Anwar and Yuan (2019), who, in their pilot study, found that employees in an organisation with explicit cybersecurity policies felt much more assertive about the importance of security breaches than those whose companies either did not have an explicit security policy or did not know if their company had one. Cram, Proudfoot, and D'Arcy (2020) posited three cybersecurity policies, the first being enterprise cybersecurity policies, which are usually high-level documents that describe the strategic direction of security initiatives within an organisation. The second is technical policies that define specific standards and procedures that operational staff should use to configure and maintain the security posture of IT resources.

The third is specific policies which detail the guidelines, rules, and procedures for employees to adhere to for IT resources and processes. ISO 27001:2013 posited that an information security policy aims to provide management direction and support information security by business requirements and relevant laws and regulations. The policy document produced from the security policy should be approved by management and shared with employees to provide a guideline for how they should carry out their roles within the scope of the policy. This is also supported by the NIST framework that provides different security policies for employees, ranging from acceptable user behaviour policies to security response plan policies (SANS Institute, 2021; ISO/IEC, 2013). Cybersecurity policies play a critical role in securing organisations and providing guidance for practitioners within organisations. Until recently, South Africa did not have adequate national policies to govern cybersecurity. The slow pace of policy creation and adoption could be credited to the complex and cumbersome process that law-making in South Africa follows.

Chigada and Kyobe (2018) stated that the process of law-making in South Africa involved six steps, namely: **1)** Introduction of the Bill in the National Assembly (NA) or National Council of Provinces (NCOPs). The NCOP ensures that provincial legislative issues are considered in the national sphere of government. Still, both legal bodies are expected to bring various legal systems to work together towards a unity of purpose; **2)** the Bill is referred to relevant Portfolio Committees and published in the Government Gazette for public comments; **3)** Committees debate and amend the Bill; **4)** Bill is submitted to a sitting house for further debates; **5)** Bill is transmitted to the other house for concurrence; **6)** President of the republic approves the Bill; **7)** The signed Bill becomes an Act of Parliament/the law of the land. They further stated that these steps often lead to inconsistencies, gaps, and misalignment in the law-making process, so they proposed a conceptual model that would lead to an effective and aligned NCPF.

Only recently, through the NCPF, Cybercrimes Act, and Protection of Personal Information Act, firm cybersecurity policies were adopted in South Africa. The purpose of the NCPF was to create a secure, dependable, reliable, and trustworthy cyber environment that facilitated the protection of critical information infrastructure while strengthening shared human values and understanding of cybersecurity in support of national security imperative and the economy (Republic of South Africa, 2015). The policy framework sets out to achieve this through centralising the coordination of cybersecurity activities and establishing relevant structures, policy frameworks and strategies in support of cybersecurity, fostering cooperation between the South African government, the private sector and civil society, thereby promoting international collaboration, developing requisite skills, research and development capacity, promoting a national culture of cybersecurity and promoting compliance with operational cybersecurity standards (Republic of South Africa, 2015).

The Cybercrimes Act, on the other hand, sets out to "create offences which have a bearing on cybercrime; to criminalise the disclosure of data messages which are harmful and to provide for interim protection orders; to further regulate jurisdiction in respect of cybercrimes; to further regulate the powers to investigate cybercrimes; to further regulate aspects relating to mutual assistance in respect of the investigation of cybercrimes; to provide for the establishment of a designated Point of Contact; to further provide for the proof of certain facts by affidavit; to impose obligations to report cybercrimes; to provide for capacity building; to provide that the executive may enter into agreements with foreign states to promote measures aimed at the detection, prevention, mitigation and investigation of cybercrimes; to delete and amend provisions of certain laws, and to provide for matters connected in addition to that." (Republic of South Africa, 2021).

The Protection of Personal Information Act (POPIA) had the objective of promoting the protection of personal information processed by public and private bodies, introducing certain conditions to establish minimum requirements for the processing of personal data, providing the establishment of an Information Regulator to exercise certain powers and to perform specific duties and functions in terms of the Act and the promotion of access to Information Act, 2000; to provide the issuing of codes of conduct; to provide for the rights of persons regarding unsolicited electronic communications and automate decision-making and to regulate the flow of personal information across the borders of the Republic of South Africa, as well as to provide for matters connected in addition to that (Republic of South Africa, 2013). The Act also set out to regulate and align with international standards about the processing of personal information by public and private bodies in a manner that gives effect to the right to privacy, subject to justifiable limitations that are aimed at protecting other rights and vital interests (The information regulator of South Africa, 2021)

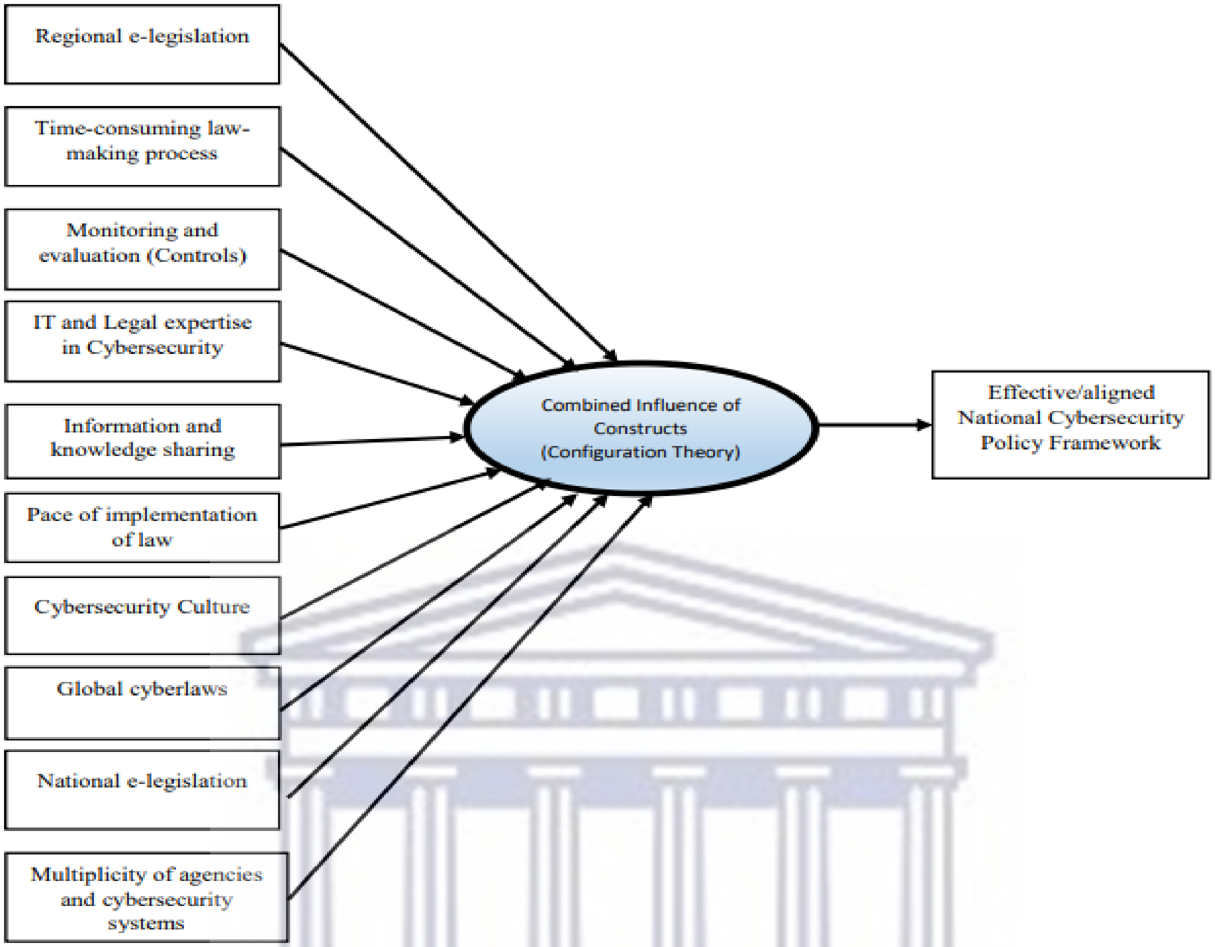

Regional e-legislation
Time-consuming law-making process
Monitoring and evaluation (Controls)
IT and Legal expertise in Cybersecurity
Information and knowledge sharing
Pace of implementation of law
Cybersecurity Culture
Global cyberlaws
National e-legislation
Multiplicity of agencies and cybersecurity systems
Combined Influence of Constructs (Configuration Theory)
Effective/aligned National Cybersecurity Policy Framework

Figure 2.7 A Configuration approach to alignment of National Cybersecurity Framework. Source (Chigada & Kyobe, 2018)

2.5.3 Cybersecurity Frameworks

Cybersecurity frameworks for the financial sector have been developed as the number of attacks on financial institutions has increased in the last few years. Frameworks include the NIST and the CSF, the International Organisation for Standardization (ISO) ISO 27001/ ISO 27002, the Open Information Security Management Maturity Model (O-ISM3), and the Centre for Internet Security (CIS) Controls that exist for the financial sector. Donaldson, Siegel, Williams and Aslam (2015) compared multiple frameworks to identify similarities and differences. The common thread running through each framework allows the implementer to identify threats, protect assets, detect threats, respond to attacks, and recover from attacks. Alexander and Panguluri (2017) described how cybersecurity frameworks, at their core, should provide the necessary CIA to information assets in institutions.

Alexander & Panguluri (2017) explored two common cybersecurity frameworks: the National Institute of Science and Technology (NIST), the Cybersecurity Framework (CSF), and the ISO 27001/ISO 27002. The NIST and the CSF are a set of everyday cybersecurity activities across the critical infrastructure sector. The framework presents industry standards, guidelines, and practices that allow communication of cybersecurity activities and outcomes across the organisation from the executive to the implementation/operations level. Figure 2.8 shows the core elements of the NIST Framework. The ISO 27001/ISO 27002 frameworks/standards describe an Information Security Management System (ISMS) and detail the steps involved in the establishment of such a system, with the ISMS aiming to minimise risk and ensure business continuity by limiting the impact of security breaches through creating policies and procedures to manage a business's sensitive information.

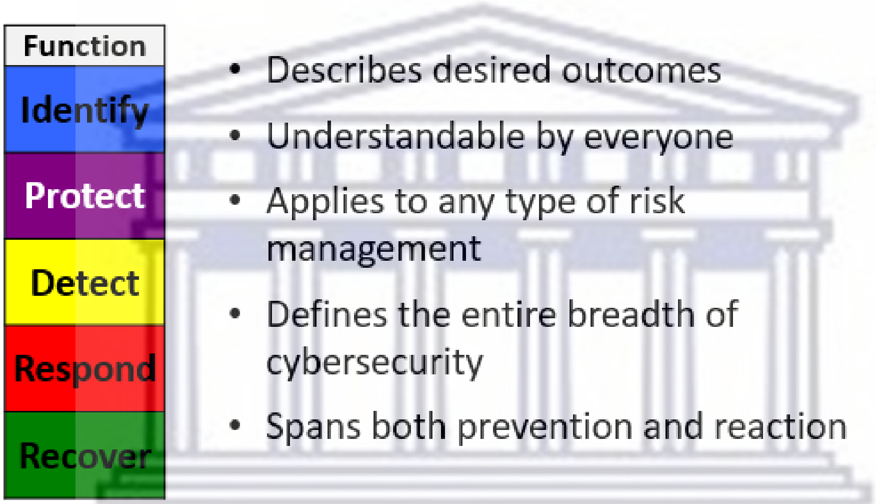

Function
Identify
Protect
Detect
Respond
Recover
• Describes desired outcomes
• Understandable by everyone
• Applies to any type of risk management
• Defines the entire breadth of cybersecurity
• Spans both prevention and reaction

Figure 2.8 NIST Framework Core. Source (National Institute of Standards and Technology, 2018)

The Open Group Information Security Management Maturity Model (O-ISM3) is a fully process-based approach to information security management and maturity, on the basis that every control needs a process for managing it. It breaks information security management down into a comprehensive but manageable number of processes, with specifically relevant security controls identified within each process as an essential subset of that process (The Open Group, 2011). ISM3 defines three fundamental principles that are used in the framework. The principles are Process, Capability, and Maturity. Through dependency analysis, ISM3 can produce a list of security objectives that form the basis for the ISMS's design, implementation, and monitoring. These objectives state explicitly how information security contributes to business objectives (The Open Group, 2011).

CIS Controls are a prioritised set of actions that collectively form a defence-in-depth set of best practices that mitigate the most common attacks against systems and networks (Center for Internet Security, 2019). The CIS Controls are technology-aimed controls developed from actual attacks. They are meant to reinforce existing security controls and serve as guidelines for managing the technology estate of an organisation.

The controls can be applied to three implementation levels: Implementation Groups (IGs). These groups are defined based on the size of the organisation and the amount of cybersecurity expertise dedicated to protecting IT assets and personnel (Center for Internet Security, 2019).

The Committee on Payments and Market Infrastructures and the International Organisation of Securities Commission (CPMI-IOSCO) proposed a set of cyber resilience guidelines for principal financial markets infrastructure, which are international standards for payment systems, central securities depositories, securities settlement systems, central counterparties, and trade repositories. These guidelines are centred around governance, the framework for comprehensive management of risks, settlement finality, and operational risks.

The guidelines aimed to maintain and promote the financial stability of financial markets' infrastructures. In the guidelines, cyber risks were acknowledged as critical risks faced by financial institutions. One of the principles set out therein was that financial institutions should identify plausible sources of operational risk from both an internal and external perspective and should mitigate their impact by using appropriate systems, policies, procedures, and controls (Bank for International Settlements and International Organization of Securities Commissions, 2016). It also stated that systems should inherently be designed with the highest security and operational reliability. The designs of systems should encompass (i) governance, (ii) identification, (iii) protection, (iv) detection, (v) and response and recovery, and these components should be driven by testing, situational awareness and, learning and evolving. Figure 2.9 depicts the components of the cyber resilience design proposed by CPMI-IOSCO.

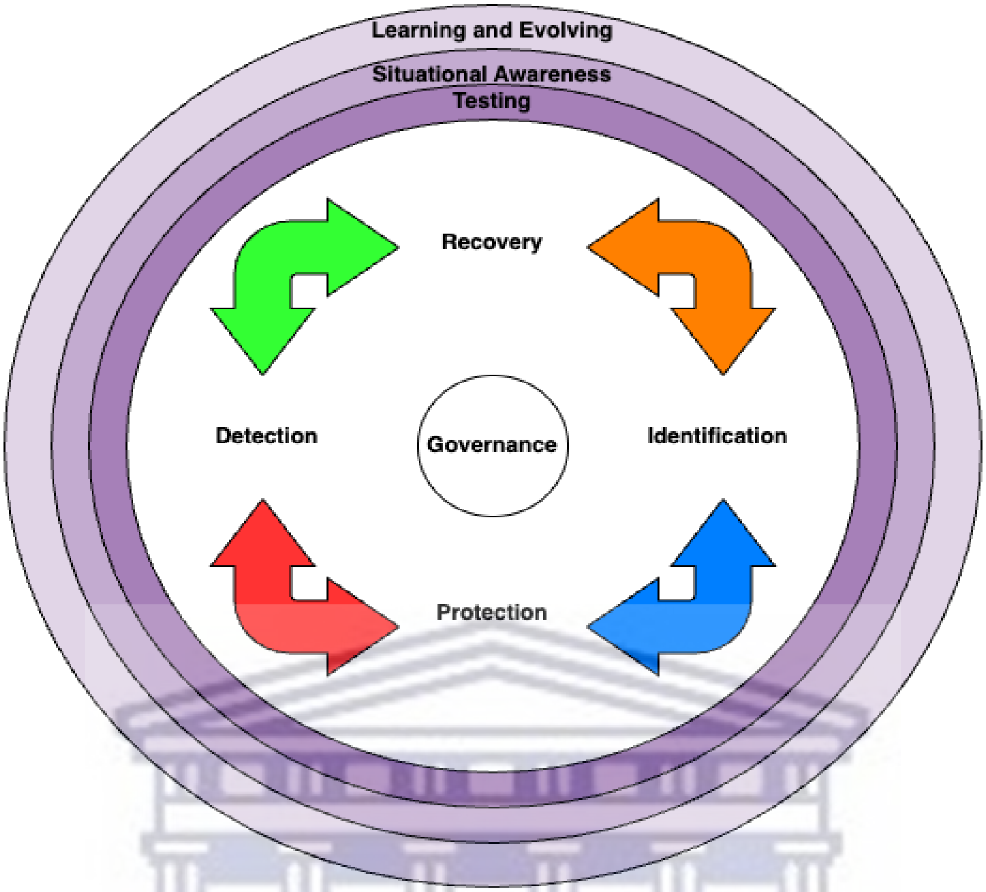


Figure 2.9 Cyber resilience guidance components. Source (Committee on Payments and Market Infrastructures Board of the International Organization of Securities Commissions, 2016)

The Financial Sector Conduct Authority (FSCA) and the South African Reserve Bank, which serves as a prudential authority, published a draft intending to create a joint standard of cybersecurity and cyber resilience for financial institutions in South Africa. Due to the ever-increasing cyber threat landscape, the proposed standard may be viewed as a response by the financial sector's regulatory bodies in South Africa. The standards aim to protect financial institutions from increasingly frequent and sophisticated cyber-attacks by proposing that financial institutions implement security controls that are commensurate with their risk appetite, based on the nature of the organisation, develop a reporting framework for cyber incidents and continuously ensure that they maintain the highest standards of cyber hygiene (Financial Sector Conduct Authority and the South African Reserve Bank, 2021).

2.5.4 Cybersecurity Tools

Cybersecurity is a computer-based discipline that deals with the presence of adversaries, and as such, to deal with these adversaries, a combination of tools is needed. These might be technical tools, processes, and practices designed to protect information systems and data from attack, damage, or unauthorised access. The protection of computer systems is the sum of prevention, detection, and response (Möller, 2020). These tools, processes and practices include but are not limited to the following:

The Security Operations Centre (SOC): Security operations are essential to an organisation's cybersecurity programme. The SOC is focused on identifying threats, vulnerabilities, and anomalies and responding to those of interest. Within the SOC, four elements help secure an organisation: threat intelligence, vulnerability management, security monitoring, and incident response. Figure 2.10 depicts how these elements feed data to each other in a clockwise direction. Below is a concise description of each of the components within the SOC.

- *Threat Intelligence and Threat Hunting:* Threat hunting is the process of proactively searching for cyber threats that may be undetected within an organisation's network. It is used to discover new TTPs used by threat actors. It employs multiple sources of information, such as endpoint detection and response (EDR) data and known indicators of compromise (IOCs), to uncover new TTPs (Ajmal, Shah, Maple, Asghar & Islam, 2021). On the other hand, threat intelligence is consumed on an operational level to generate alerts against threat indicators in real time. The intelligence derived from it is used with security alerts to enrich the detection and alerting process. It is also helpful during cyber incident response. Threat intelligence collects data from numerous sources, such as threat-sharing groups (ISACs). Through these sources, threat intelligence feeds into vulnerability management, where the members of the SOC use the information to understand what vulnerabilities a threat actor is exploiting. It also contributes to continuous monitoring to improve detection capabilities (Thompson, 2020).
- *Vulnerability Management:* Vulnerability management comprises scanning for missing patches, misconfigured systems, and vulnerable applications and integrating vulnerability information from multiple sources. It is also concerned with understanding the missing

process that may lead to a compromise and the specific tactics, techniques, and methods used by threat actors. Based on the information gathered vulnerability management can be used to inform users within an organisation of vulnerabilities and countermeasures they can use. They can also assess an organisation's environment for weaknesses that threat actors could exploit (Thompson, 2020; Syed, 2020).

- *Continuous Monitoring:* Monitoring within a SOC works towards understanding what is happening within an organisation's environment. This can be achieved through endpoint monitoring and alerting. Rahman (2021) stated that good design and implementation of continuous monitoring provided a just-in-time reflection of users, devices, networks, data, workloads, activities, and infrastructure statuses within an organisation. It also helps with identifying intrusions.
- *Cyber Incident Response:* Cyber incident response is a structured approach to identifying, containing, and minimising the cost of a cyber-attack or a live incident. During an incident response process, the SOC and all those affected by the cyber incident will go through identification and containment phases to identify all infected endpoints. Eradication is the process of removing the infection from the environment and endpoints. Recovery occurs once the affected endpoints have been cleaned up and patched, and lessons have been learnt by retrospectively looking at what happened during the incident and seeing what could be done better (Thompson, 2020; EC-Council, 2021).

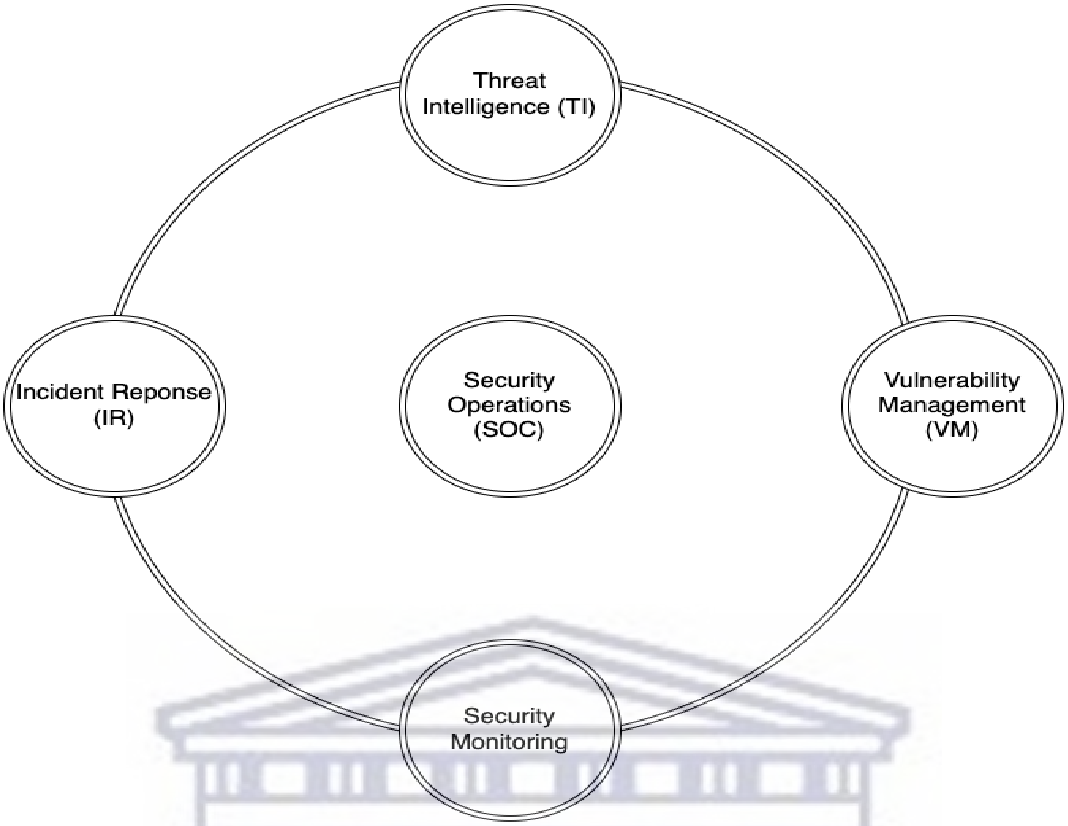


Figure 2.10 Components of security operations. Source: Thompson, 2020

The Confidentiality, Integrity, and Availability (CIA) Triad: The fundamental principles of information security encompasses confidentiality, integrity, and availability. These three principles are the standard guiding policies for cybersecurity within organisations, and they often inform the main objective of any cybersecurity programme (Möller, 2020). Confidentiality is concerned with recipients of information. Management should ensure that only people who are authorised to access information can access it. Integrity ensures that data is stored and presented strictly as intended without tampering; availability ensures that data can be immediately accessed (Klonoff, 2015). Figure 2.11 depicts the triad.

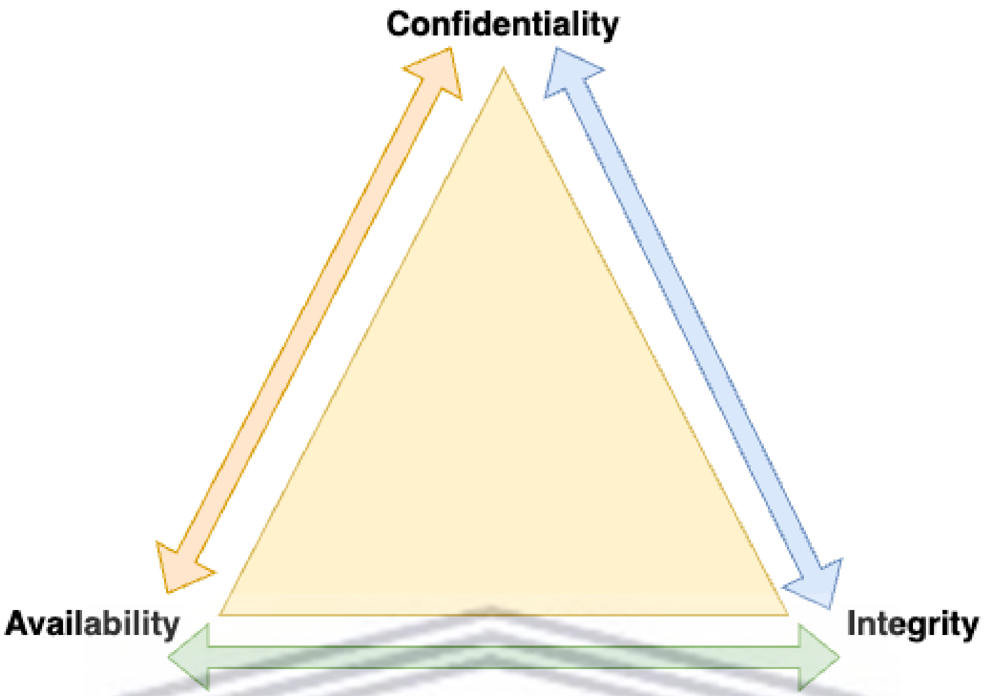


Figure 2.11 CIA Triad. Source Author 2023

Cybersecurity Training and Awareness: The importance of educating organisational end-users about their roles and responsibilities towards information security is widely acknowledged (van Niekerk & von Solms, 2013). Such education is needed because, intentionally or through negligence, or often due to a lack of knowledge, employees are the greatest threat to corporate information security (Mitnick, Simon, & Wozniak, 2002). Furthermore, when organisations raise awareness about cybersecurity, there is bound to be less conflict of interest between business and security objectives, thus leading to better performance and more benefits than security (Wood, 2008).

Intrusion Detection and Prevention Systems (IDS/IPS): Intrusion prevention systems are a combination of software and hardware tools designed to detect and prevent malicious attacks on organisational networks. They are deployed on an organisation's network to monitor and locate malicious traffic by analysing the electronic signatures of already determined attacks.
When matches are detected, the IPS terminates the network connection (Baykara & Das, 2018). Hammad, Hewahi & Elemdany (2021) supported Baykara and Das (2018) by stating that the primary responsibilities of (IDS/IPS) were to monitor network activity, audit network and system configurations for vulnerabilities, and analyse data to prevent attacks.

Security Risk Analysis: Information risk incorporates cybersecurity risks from threat actors who exploit vulnerabilities and IT operation risks from operator error to IT component breakage. Risk analysis enables organisations to identify the potential risks affecting them adequately, prioritise the defence of their digital assets, and determine the necessary security controls to be implemented. This is often achieved by employing cybersecurity models, compliance frameworks and standards that rely on matrices to categorise everything effectively (Blum, 2020; Insua, Couce-Vieira, Rubio, Pieters, Labunets & Rasines, 2019).

2.5.5 Cybersecurity Culture

Attacks, breaches, and incidents represent significant challenges to organisational culture. The fact that an attack has occurred often creates a climate of uncertainty, feelings of vulnerability, and inadequacy on the part of the attack (ISACA, 2013). The number of cybersecurity incidents reported globally has increased recently. Advancements in algorithms, information systems, machine learning, artificial intelligence, and increased spending on cybersecurity are inadequate for securing information systems and digital assets for organisations. It has become apparent that the human aspect of cybersecurity warrants deeper investigation and understanding, not only in terms of impacts on organisations, communities, and individuals, but also on how human behaviour and culture contribute to cybersecurity-related incidents (Jeong, Oliver, Kang, Creese, & Thomas, 2021). Keman and Pearlson (2019) stated that insider threats from human behaviour are one of the most challenging aspects of security control. Building a culture of maintaining cybersecurity within an organisation guides employee behaviour and increases cyber resilience. This is because the cultural view around cybersecurity in an organisation plays a huge role in the effectiveness of the security controls and employees' inclination to adhere to these controls.

Knowles (2016) stated that the moral principles that govern a person's behaviour are critical to any sound cybersecurity defence strategy. Rao and Herath (2009) pointed out that their peers' behaviour influences employees' cybersecurity behaviours as intrinsic or extrinsic motivators. Factors such as an employee's desire to complete a task at any cost also play an essential role in their behaviour and perception of cybersecurity. Pfleeger and Caputo (2012) supported this by stating that when security interferes with a task, a person may ignore or even subvert security since the person is rewarded for the primary task more than for maintaining security.

Definitions of cybersecurity culture, information security culture and security culture are often intertwined. Still, the basis of most of the definitions seems to agree with the definition of Dhillon (1997), who described security culture as the 'totality of human attributes such as behaviours, attitudes and values that contribute to the protection of all kinds of information in a given organisation.' Martins and Eloff's (2002) definition posited security culture as an 'assumption about perceptions and attitudes that are accepted to incorporate information security characteristics, as to how things are done in an organisation', supporting the notion that human behaviour and attitudes contribute to information security culture. Alshaikh (2020, p. 1) then defined cybersecurity culture as 'contextualised to the behaviour of humans in an organisational context, to protect information processed by the organisation through compliance with information security policy with an understanding of how to implement requirements cautiously and attentively; as embedded through regular communication, awareness, training and education initiatives'.

Uchendu, Nurse, Bada, and Furnell (2021) stated that the key themes within the definition of information security culture between the years 2010 and 2020 included employee behaviour, human characteristics, the attitudes of employees, organisational culture and security awareness, which were described as the conditions under which users within an organisation are both committed to and aware of the company's security mission (Siponen, 2000). It was also apparent that cybersecurity culture within organisations is influenced by internal and external factors, with internal factors being those within the control of the organisations and external factors being those within which the organisations exist or which they do not have control over. Uchendu *et al.* (2021) highlighted internal factors that influence cybersecurity culture as support and leadership from top management, clear policies and procedures for employees to understand and abide by, security awareness and training programmes, and the management of change. *Da* Veiga, Astakhova, Botha & Herselman (2020) supported Uchendu *et al.'s (2021) views by stating that the four main internal factors influencing cybersecurity culture* are organisational, management, human, and mutual trust. Those four main factors include Security Education, Training and Awareness (SETA), policies and procedures, the life cycle state of the organisation, and management. From an external perspective, da Veiga *et al.* (2020) posited that the external factors influencing cybersecurity culture are national culture, political and legal, economic, sociocultural, and technical and technological factors. Table 2.2 provides a detailed overview of the factors that could influence cybersecurity culture.

Although the South African government has noted cybersecurity and a cybersecurity culture as essential for national security, the government has lagged in implementing the necessary legislation and policies. Although some aspects of common law offences within the constitution of the Republic of South Africa were crudely applied to cybersecurity, it was not until recently that the country adopted the NCPF (Republic of South Africa, 2015), a well-set out Cybercrimes Act (Republic of South Africa, 2021), and enacted the POPIA Act (Republic of South Africa, 2013).

The South African Cabinet only adopted the NCPF in March 2012 to respond to the country's cyber threats. The Cybersecurity Crimes Bill, although first published in 2015, was only adopted and signed by the president of the republic on the 26th of May 2021 and is still awaiting a commencement date, and POPIA, which was first introduced to the public in 2013, was only fully implemented and enforced from the 1 July 2021 (The information regulator of South Africa, 2021). All this proves the glacial pace at which cyber-aware legislation and regulation development has been taking place within South Africa, which can be viewed as a reflection of the cybersecurity culture within the country.

Mokobane and Botha (2020) found that *ubuntu*, which is part of South African culture, can influence a South African's susceptibility to social engineering, which is an act of manipulating people into performing actions or divulging confidential information that might be used for malicious purposes (Hatfield, 2018). *Ubuntu* is a South African word that defines a way of life with pillars of personhood, humanity, humanness, and morality and promotes the spirit that one should live for others (Metz, 2011). Furthermore, Du Toit, Hadebe, and Mphatheni (2018) stated that individuals lacked the appropriate awareness and understanding of cybercrimes. They faced the challenges of not knowing where to report cybercrimes and how such crimes should be reported. Some cybercrime victims felt embarrassed that they had fallen victim to cybercrime. Those victims sometimes did not share their experiences out of fear of embarrassment.

Table 2.2 Factors influencing cybersecurity culture Adapted from da Veiga, Astakhova, Botha, & Herselman (2020)

External Factors	**Internal Factors**			
National Culture	**Organisational Factors**	**Management Factors**	**Human Factors**	**Mutual Trust Factors**
Political and legal factors	The internal state of the organisation	Management	Personality and values	Mutual trust between employer and employee and between employees
	Life cycle state of organisation	Information security policies & procedures	Needs	Customer trust in the organisation
Economic Factors	Level of overall organisational culture	Information security risk management	Emotional condition	
Sociocultural factors	System protection for information	Operational management	Knowledge of information security	
Technical and technological factors	Resources	Change management	Information security compliance	
		Personal information security management	Information security compliance	
		Information security education, training & awareness		
		Security behaviour management		

2.6 Empirical Studies From Other Countries

Huang and Chiang (2021) revealed how a remote graph server geographically located in London took over forty-one automatic teller machines in Taiwan. The server evaded all the security standards established by the state-owned IS0 27001 and ISO 20000-certified bank. The attack highlighted critical flaws in security practices that were considered secure. It exposed how many preventative measures put in place by financial institutions are failing to prevent them from falling victim to intelligent cybercriminals. They further identified that some of the challenges faced by financial institutions regarding detecting modern-day cyber threats are invisible threats (zero-day vulnerabilities), structural weaknesses (infrastructure design or inherited complexity of computer architecture), human weakness, and artificial intelligence (AI) powered attacks. To overcome these challenges, they proposed a unified self-adaptive framework that would have the ability to learn about the institution’s environment and threat landscape, minimise potential exposure to vulnerabilities and utilise external input from humans within the institution to verify its actions.

To address the growing threat of cyber-attacks on financial institutions, the then governor of the state of New York in the United States of America proposed a new regulation that would require banks to develop and maintain their cybersecurity programmes by empowering the programmes to have the capability of being able to able to identify, detect, respond, and resolve cybersecurity threats (Heltman, 2016).

Van der Kleji, Schraagen, Cadet, and Young (2022) also noted how cyber threats and incident managers within the financial sector in the Netherlands face an increasing number and complexity of threats and incidents. They further posited how developing a decision support system for managers within cyber defence centres or security operation centres for financial institutions could help organisations deal with new cyber challenges. Such decision support systems would help managers keep track of more significant incidents and monitor finer details when dealing with a cyber incident. Like other countries, banks in Bangladesh are under pressure to digitise their day-to-day operations to satisfy clients and investors. This has led to abuse of some of the information systems put in place by the banks, which has led to cybercrimes such as cyber laundering occurring within the Bangladeshi banking environment. Joveda, Khan, and Pathak (2019) ran a study to create a cybersecurity system for detecting money laundering within the Bangladeshi banking sector. They did this by investigating the financial frameworks within the country for any self-evident weaknesses that cybercriminals could exploit. From that investigation, they created a list of recommendations for the banking sector in Bangladesh, including developing IT infrastructure, IT governance, and state-sponsored cybersecurity initiatives and encouraging continuous research and development of new security systems for the banks.

2.7 Gaps In The Literature

We have identified some gaps that should be addressed by analysing the literature on cybersecurity, cybercrime, and the effects of cybercrime on the South African economy. The literature review did not adequately cover cybersecurity and cybercrimes within the banking sector in South Africa. Most of the literature on cybercrimes within the banking sector in South Africa is based on the findings of a report published by SABRIC. Apart from that source, not much has been publicised about cybercrimes and their effects on the banking sector. Furthermore, we found that the literature available about cybersecurity and cybercrime within the country took a broad view and did not adequately address the challenges faced by commercial banks or shed sufficient light on the complexities faced by commercial banks who were trying to protect their digital assets and information systems from cyber threats within the country.

The cybersecurity frameworks identified in the literature do not cover the scope of the commercial banking sector in South Africa—those analysed usually refer to internationally recognised standards and frameworks such as NIST CSF and ISO 27001. Furthermore, there was a gap in cybersecurity information and incident reports from commercial South African banks. The lack of literature on cybercrime suffered by the banks makes it more challenging to gain insight into some of the challenges commercial banks face. Due to the researcher's limited knowledge and the constrained timeframe of the study, he was unable to find sufficient literature that addressed the question of the direct impact of cybercrimes on the economy of South Africa and how commercial banks have responded to the threats posed by cybercrimes, given the unique challenges they face. By analysing the literature and through consultation with a wide range of sources, the researcher identified gaps that served as the basis for developing a conceptual framework for commercial banks that would address some of the challenges they face within the cybersecurity domain. These gaps are presented in Table 2.3 Gaps identified in the literature.

Authority/Study	South Africa’s Response to Cybersecurity	Cybersecurity Landscape in South Africa	Cybersecurity Incidents Within Banks in South Africa	Cybersecurity Within the South African Banking Sector	Cost of Cybercrimes to the South African Economy and Banking System	South African Cybersecurity Frameworks for Commercial Banks	Cybersecurity Culture in South Africa	Cybersecurity Challenges in South Africa
Accenture South Africa, 2020	x	x						
Van Niekerk B., 2017		x	x					
INTERPOL, 2021		x						x
Republic of South Africa, 2015 **Republic of South Africa, 2021** **Republic of South Africa, 2013**	x							
Chigada & Kyobe, 2018	x	x						
South African Banking Risk Information Centre (SABRIC), 2019		x	x	x	x			
Ramluckan, van Niekerk, & Leenen, 2020		x						x
Mbelli & Dwolatzky, 2016		x						x
Mothibi & Amali, 2018								x
Mokobane & Botha, 2020							x	x
Musoni, 2019	x							
Du Toit, Hadebe, & Mphatheni, 2018							x	x

Table 2.3 Gaps identified in the literature.

* ☒ Represents what has been covered in the study

2.8 Chapter Summary

This chapter introduced the banking landscape within South Africa, as well as the new entrants into the banking landscape that are bringing with them innovation and a charge towards digital-first banking. It also discussed fintech and how older banks integrate these fintechs into their ecosystems or innovate internally. It also examined the literature on cybersecurity, its varying definitions, and the differences between information security and cybersecurity. Using the ITU definition of cybersecurity, the chapter investigated the various aspects that cybersecurity encompasses. These aspects were tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies.

The literature on legislation regarding cybersecurity and cybercrimes in South Africa was also examined. The literature explored the South African government's stance towards cybersecurity and cybercrimes and the cybersecurity culture present within the country. It was evident that although cybersecurity was a concern for the government, the adoption and implementation of new cyber legislation was slow and lagged behind that of other countries. Furthermore, the challenges and factors contributing to cybersecurity within South Africa were identified through the literature and information available about previous significant and impactful cyber incidents within the country. The subsequent chapters deal with cybersecurity challenges within and in the country's banking sector. The next chapter addresses some common cybersecurity frameworks available to commercial banks within the country. It shows how they fail to address some of the shortcomings identified in the literature.

Chapter Three : Theoretical Framework

3.1 Introduction

This chapter presents and expounds on the theoretical frameworks and models that guided the study. The chapter overviews each framework and shows how it contributed to the study. Secondly, it highlights gaps identified within the theoretical frameworks, and thirdly, it proposes a conceptual framework to address these gaps. Finally, the chapter concludes with a summary of the chapter. Ocholla and Le Roux (2011) described theoretical frameworks as explicit statements of a hypothesis or theoretical assumptions based on a research study and the research methods that guide researchers when they test the study's assumptions. Their views were further supported by Grant and Osanloo (2014), who posited that a theoretical framework is a foundation from which all knowledge is constructed for research. It serves as a support structure for the rationale for the study, the problem statement, the purpose, the significance, the objectives, and the research questions. The study considered five theoretical frameworks: the NCPF, systems theory (systems thinking), complexity theory, and chaos theory. The frameworks are discussed below.

3.2 Theoretical Frameworks That Informed The Study

3.2.1 National Cybersecurity Policy Framework

The NCPF was adopted in this study as it forms the bedrock of cybersecurity at a national level within the country. The policy framework offers a guideline on how to deal with cybersecurity and on the steps taken by the government to address the ever-present cyber threat. The policy framework was the South African government's response to the numerous cyber-attacks that have occurred in recent years. The framework was developed to aid the government in responding to the present cybersecurity threat by supporting capabilities that effectively coordinate departmental resources to achieve standard cybersecurity safety and security objectives (Republic of South Africa, 2015). The framework aims to create a secure, dependable, reliable, and trustworthy cyber environment that supports the protection of critical infrastructure. The policy framework also calls for coordinating cybersecurity activities between key stakeholders in the country. These stakeholders include the private, public, and civil society. Additionally, the NCPF provides a national verification system to independently assess and certify products and systems used to process or store information that might impact national security. Furthermore, The NCPF advocates for a strong cybersecurity culture within the country. It tasks civil society, government and the private sector with driving cyber awareness and creating a positive narrative around cybersecurity within the country (Republic of South Africa, 2015). The country is still vulnerable to cyber-attacks due to its narrow and fragmented approach to cybersecurity. Bramwell (2017) stated that although the NCPF established the National Cyber Security Advisory Council (NCAC) on October 15, 2013, the NCAC was still developing national CSIRTs. That further highlighted the slow pace at which the policy framework has been implemented. Ntsaluba (2017) posited that although the NCPF made significant provisions for state organs to collaborate and develop security measures to ensure the safety of critical infrastructure under their respective portfolios, this has yet to lead to tangible solutions being developed by various organs of state to highlight the inefficiencies of the government in responding to cyber-attacks.

Currently, commercial banks in South Africa use the NCPF as the bedrock of any cybersecurity initiatives undertaken by the banks and their stakeholders. The NCPF informs cybersecurity at a national level, and as such, any cybersecurity strategies and advancements made by commercial banks need to uphold and align with the NCPF. SABRIC, which most commercial banks are members of, established a CSIRT to aid banks in information sharing around security threats and in responding to cyber incidents in the financial services sector in South Africa. SABRIC strives to remain strategically aligned with the NCPF and supports any efforts put forward by the NCPF (South African Banking Risk Information Centre (SABRIC), n.d.). The NCPF further entrenches itself into the banking domain by assigning the responsibility of preventing, investigating, and combating cybercrimes in the Republic to the Department of Police and the SAPS (Republic of South Africa, 2015). The shortcomings of the NCPF are that although it makes significant advances in improving the country's cybersecurity posture, it places the responsibility of preventing, investigating, and combating cybercrimes on organs of the state that are plagued by inefficiencies, understaffing and a lack of expertise when it comes to cybercrimes (Aphane & Mofokeng, 2021; Sicetsha, 2018). It provides thoughts and suggestions for tackling the persistent cybersecurity threat. Still, it does not give the private sector, civil society, or state organisations an implementation plan. Regarding the banking sector, it relies heavily on the capabilities of SABRIC, a non-profit organisation established by banks. Additionally, the NCPF is affected by the lack of service delivery by the South African government. Although the policy framework has existed since 2015, some of its suggestions were only implemented years after the policy framework was made public. The Cybercrimes

Act, which would enable the persecution of cybercrimes, was only signed by the republic's president on 26 May 2021. The POPIA, which protected personal information as stipulated by the NCPF, only came into full effect on 1 July 2020. Sutherland (2017) also decried that although the policy has borrowed elements from Europe and the US, little effort has been put into adapting the borrowed elements to the South African landscape. Bote (2019) further argued that the NCPF lends itself more to being a framework than being a policy, and it is primarily a framework for thinking and policymaking on cybersecurity for the various state agencies.

3.2.2 Systems Theory

‘The whole is greater than the sum of its parts’ Aristotle. Wilkinson (2011) defines systems theory as a conceptual framework based on the principle that parts of a system can best be understood in terms of relationships with each other and other systems rather than in isolation. Based on the definition of cybersecurity provided by the International Telecommunication Union, it is evident that cybersecurity comprises multiple parts. As such, addressing the challenges in the field requires an approach that considers all the individual components. Dekkers (2017) posited those systems theories emerged in the first half of the … (something is missing here) as a response to the need to construct more complex systems coherently. He stated that systems theory comprises five basic concepts, namely:

- Systems – A system consists of distinct elements within the total reality (universe), defined by the researcher’s aims. All the aspects of reality have at least one relationship with the other elements and may have one-to-many relationships with other elements in the universe (Dekkers, 2017).
- Elements – These are the minor parts needed for the purposeful analysis of a system (Dekkers, 2017).
- Relationships – describe the dependencies between elements. These relationships may be monodirectional, bidirectional or multidirectional (Dekkers, 2017).
- The Universe – comprises all the elements and their known and unknown relationships (Dekkers, 2017).
- The Environment –any part of the universe that has known direct relationships with the elements within the system (Dekkers, 2017).

Figure 3.1 depicts a system with the five concepts Dekkers (2017) identified. The rectangular items in the figure are elements within a system, and the solid lines between the elements depict the relationships between the components. The dotted line represents the boundary between the internal and external parts of the system. Applying systems theory to cybersecurity may include using systems thinking, a subset of systems theory. Amissah, Gannon and Monat (2020) described it as an approach to reasoning and treatment of real-world problems based on the notion of a system to understand the relationships between components and their overall intentional or unintentional impact on the system.

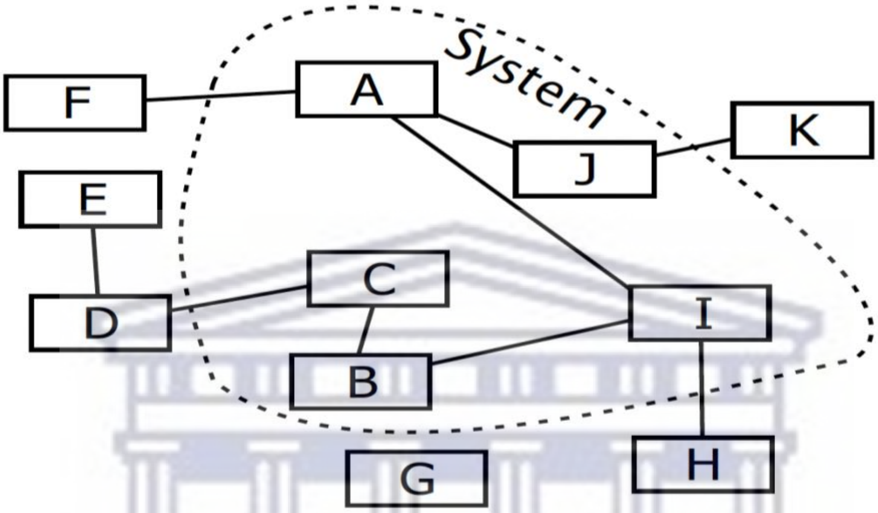


Figure 3.1 System with elements, relationships, and boundaries. Source: (Dekkers, 2017)

When applying systems thinking to cybersecurity, Savage and Schneider (2009) posited that security is a holistic problem. It is a property of a system and not just of its components; a small change to any of the elements within the system could have catastrophic consequences for security. Security aspects include people, processes, and technology, with each component comprising more minor elements. Salim And Madnick (2016) posited that a novel approach to addressing risk needs to be adopted, given the nature of security risks in today’s ever-changing risk (threat) environment. They opined that employing systems that employ thinking and address cybersecurity threats through technical approaches could incorporate people and management as elements of a holistic cybersecurity strategy. As part of a complex system, Yan (2020) identified the characteristics of cybersecurity as follows:

- Complex – The complex nature of cybersecurity is due to the diverse security issues and the diversity of influencing factors.
- Unpredictable – The interactions between the elements (people, processes, and technology) are often unpredictable and complex. Also, the techniques used by

attackers are often unknown and unexpected as attackers employ various evasion techniques.

- Dynamic – The dynamism of cybersecurity security may be attributed to the rapidly changing state of each element that makes up a holistic system. The state of elements could change at any time.
- Asymmetric – Attackers have an advantage over defending organisations as they take time to prepare for an attack by gathering substantial surveys on the organisation by employing vulnerability scanners, intelligence gathering and weaponisation.

Systems thinking can help address the gap between the various domains (social, technical, economic, regulatory, legislative, and political) involved in cybersecurity decision-making. Furthermore, this approach to cybersecurity may be employed to establish cyber resilience in critical infrastructure (Shaked, Tabansky, & Reich, 2021; Zoto, Kianpour, Kowalski, & Lopez-Rojas, 2019). For these reasons, systems thinking was employed in the study. That made it possible to consider cybersecurity as a system whereby different elements contribute to the whole, and it further aligned with the trifold approach to cybersecurity mentioned in the literature, which comprises people, processes and technology. Systems thinking's success, however, depends upon the interaction and interdependence of elements. It relies on elements interacting and allowing the influence of other elements to alter the entire system's state to achieve a set objective (Sinnot & Rabin, 2012). However, in large organisations such as banks, silos form, due to their nature, that then form distinctions between departments and their functions (Cabrera & Cabrera, 2018). Chigada and Ngulube (2015) established that departments within banks in South Africa operated in silos, which made it hard to use knowledge sharing and knowledge management. This type of siloed approach hampers the implementation of systems thinking to solve cybersecurity problems. Additionally, systems thinking accepts elements of the system as they are. It does not alter the elements or force them to adhere to a strict state to achieve an objective. Instead, it emphasises the system's adaptability by concentrating on emerging processes rather than static structures. That approach can be detrimental to an organisation as some departments or functions(elements) sometimes need to be changed to align with the organisation's overall vision (Jansen van Vuuren, 2002; Friedman & Allen, 2014).

3.2.3 Complexity Theory

Merriam-Webster (2023) defines complexity theory as a field of study shared by mathematics and computer science that is concerned with how the computational complexity of problems increases as the number of cases involved increases, together with the classification of the issues, according to whether a solution can be found in polynomial time and to the algorithms required for such a solution. Figure 3.2 depicts the overlap of complexity theory and systems theory, showing that they share common characteristics and may be seen as complements.

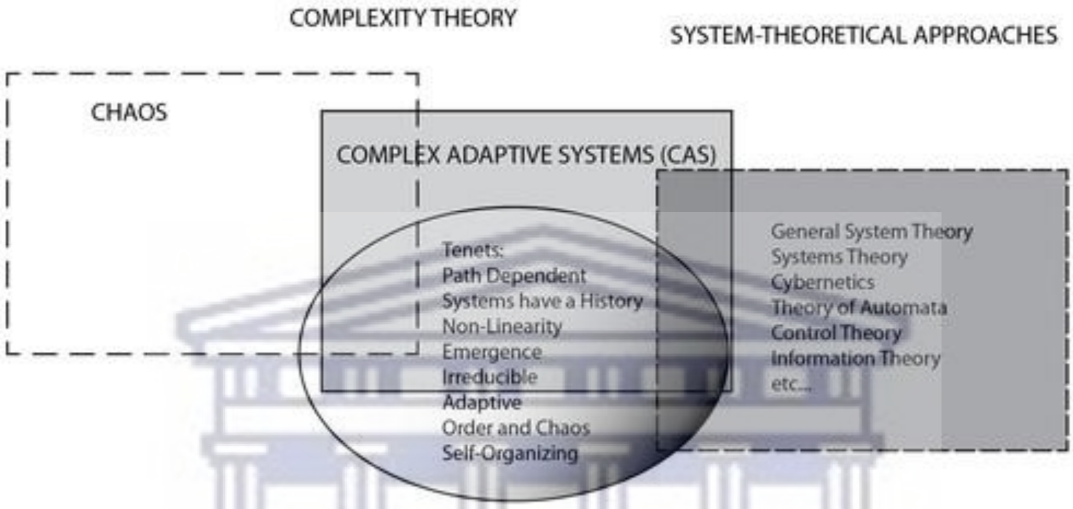


Figure 3.2 Graphical abstract of complexity theory and system-theoretical approaches. Source: (Turner & Baker, 2019)

Turner and Baker (2019, p. 9) stated that complexity theory is synonymous with complexity science and, as such, may be defined as 'A subset of all systems; a subset which is abundant and is the basis of all novelty; a subset which is evidenced in biology, chemistry, physics, social, technical and economic domains; which coevolves with its environment; a subset from which structure emerges'.

Self-organisation occurs through heterogeneous components' dynamics, interactions, and feedback. From the above definitions, complexity theory may be viewed as an extension of systems theory, with the difference being that complexity theory is concerned with a complex system in which the parts and the system and their interactions and behaviours cannot easily be explained by the constituent parts (Gandhi, 2014). Complexity may be seen as an attribute of large systems comprising numerous interdependent agents that unpredictably influence each other and behaviour. The characteristics that affect the complexity of a system are diversity, adaptiveness, connectedness, and mutual dependency of the agents in the system (Benya, Nan, Tanriverdi, & Yoo, 2020). Xu, Yung, and Wang (2021) posited that complexity theory may be applied to cybersecurity because cybersecurity is a complex problem to solve. Cybersecurity is made up of multiple factors that influence the problem. These factors include the scale of the cyberspace and threat landscape, the complexity of the interdependence and interactions between devices, humans, regulations, and laws, the adversarial skills held by attackers, which are often equal to those of the defenders, the challenges in quantifying the extent of the cybersecurity, and the multidisciplinary nature of cybersecurity. Brantly (2019) further supported the notion of applying complexity theory to cybersecurity by stating that complexity theory has the potential to shift policymakers from concepts of linear determinism to non-linearity and, eventually, non-deterministic modelling. This is so because the laws and policies being developed for cybersecurity are currently trying to address an ever-changing environment and often overlook the impact of complexity on potential outcomes. Although offering novel and valuable approaches to cybersecurity, complexity theory may not be considered a silver bullet to cybersecurity because it is a complex theory to apply in practice and is computationally intensive, making it harder to apply to large and complex computer networks. Furthermore, it does not provide a way to accurately predict the behaviour of complex systems because of the nature of non-linear interconnected systems.

Armstrong and Mayo (2009) stated that complexity theory falls short in natural world cyber systems and organisations, as it requires the ability to model and simulate these complex systems with various stakeholders such as regulatory bodies, investors, customers, and extensive information systems often spanning geographical locations; which is the case for South African banks. Locally, banks do not exist in silos. For complexity theory to be practical, it must account for the various relationships between the banks, regulatory bodies, government, corporate partners, civil society, and their internal departments. However, as Chigada and Ngulube (2015) and Chigada (2021) stated, there are silos within banks and governmental departments, which makes it challenging to implement complexity theory fully. Additionally, complexity theory would not be able to provide a long-term strategic approach to managing cybersecurity in the banks because the theory is more concerned with the system and how the introduction of change would affect it; so, it does not aspire to a stable and predictable state (Smith, 2004; Levy, 2000)

3.2.4 Chaos Theory

Chaos theory, which the famous butterfly effect has popularised, opines that flapping a butterfly's wings in a different part of the world could cause a storm in another part of the world. Chaos theory may be defined as a system's apparent lack of order because systems rely on their being an underlying order. The slightest change to the system and events may cause changes throughout the system (Lorenz, 1961, as cited in Chigada & Kyobe, 2018). McBride (2005) stated that chaos theory is a subset of complexity theory. However, it concerns non-linear dynamic systems whose behaviour does not follow predictable and repeatable pathways and systems that do not manifest any fixed or deterministic outcomes. Their views are further supported by Turner and Baker (2019), who highlighted an overlap between chaos, complexity, and systems theories. McBride (2005) further stated that chaos theory is made up of key concepts, which are mentioned below and depicted in Figure 3.3. The domain of interaction – The interaction domain encompasses all possible states a system could be in.

- Initial conditions – A system or organisation's initial state is where the change being studied occurs.
- Strange attractors – These are the characteristics, dynamics, and known patterns of behaviour that systems and entities within the domain of interaction exhibit over time.
- Events and choices – These represent the actions taken by actors within the system.
- Edges of chaos – These are internal or external events and decisions made by actors within the system that change the system's state from stable to a point where any change introduced in the system might result in chaotic behaviour.
- Bifurcations – These are qualitative changes in the behaviour of a system.
- Connectivity – Connectivity is the relationship between all known entities within the interaction domain.

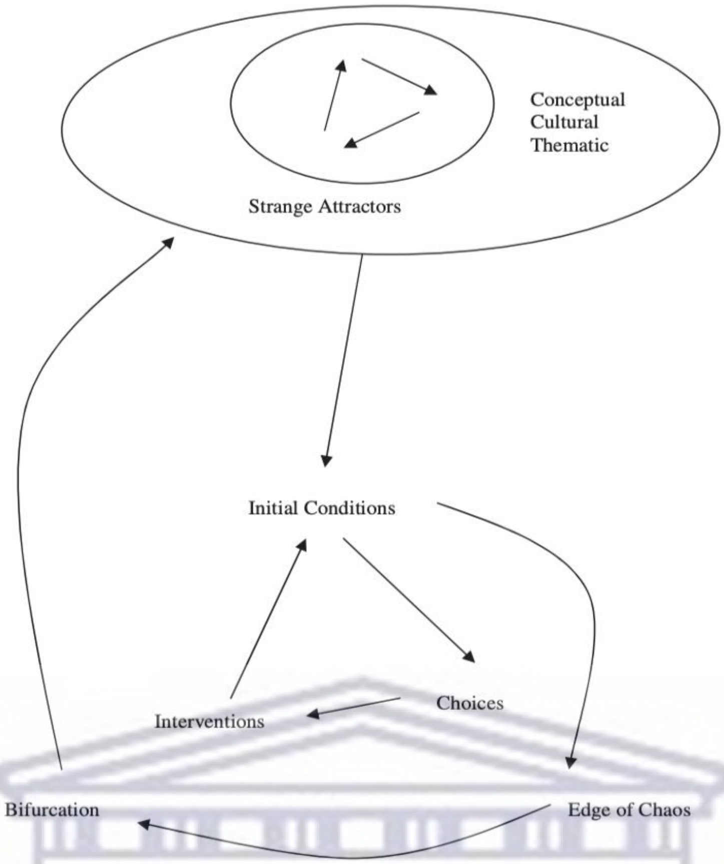


Figure 3.3 Cycle of chaos. Source (McBride, 2005)

Raphael, Célestin, and Djiethieu (2019) posited that chaos theory may be applied to complex security problems to find optimal solutions and make systems more secure. This is because chaos theory enables organisations to look at security as a non-linear phenomenon and thus apply an approach that would bring order and structure to an otherwise complex environment.

McLeod, Dorantes, and Dietrich (2008) stated that chaos theory seeks to find an underlying order in the unordered external behaviour of dynamic systems. It may be employed to address security vulnerabilities and actions in organisations, which often vary and do not follow a set pattern.

Leveraging off chaos theory, organisations may overcome zero-day exploits, which usually use unknown behaviour and undisclosed vulnerabilities and are seldom detected by traditional linear analysis of security events.

Chigada and Kyobe (2018) posited that the process of law-making in South Africa can be explained by chaos theory. As such, the laws and regulations around cybersecurity within the country are impacted by the chaotic nature of the country's processes of creating rules and regulations and having those laws accepted by the Cabinet.

This often leads to misaligned laws and regulations and a delayed response to the ever-changing cyber domain. Given that the study employed the NCPF as one of its guiding theoretical frameworks, chaos theory became an applicable theory whereby cybersecurity may be approached in South Africa. This occurred because the NCPF underwent a chaotic process while becoming law in the republic.

3.3 Gaps In Theoretical Frameworks

This section discusses gaps identified in the theoretical frameworks considered for the study. The gaps and those identified in the literature review were used to inform the proposed conceptual framework. Table 3.1 below summarises the gaps in the theoretical frameworks that guided the study.

Theoretical Frameworks	Unpredictability Of The Cyber Domain	Industry Information Sharing	Cybersecurity Culture	Alignment Of Business And Cybersecurity	Practical And Enforceable Legislation	Resource Allocation	Cybersecurity Awareness	Various Contributors To Security Posture	South African Cybersecurity Frameworks For Commercial Banks
National Cybersecurity Policy Framework	x	x	x				x		
Systems Theory				x		x			
Complexity Theory					x			x	
Chaos Theory	x					x			

Table 3.1 Theoretical framework gaps

* x Represents the framework's applicability to cybersecurity

3.4 Proposed Conceptual Model

This study aimed to develop a conceptual cybersecurity framework for commercial banks to assist them in improving their security in the wake of the ever-increasing cybersecurity threat. The conceptual framework was informed by the gaps identified in the literature review, which were identified in the theoretical frameworks section to address them. Furthermore, it incorporates the NCPF, systems theory, complexity theory, and chaos theory. It adopts a lens through which entities within cybersecurity are viewed as elements of a complex and chaotic system that continuously interact with each other and transition from one state to another. The researcher was able to develop a conceptual model made up of factors that contribute to a cybersecurity framework for commercial banks. The factors represent elements within an organisation (system) that have relationships with each other and interact with each other. As depicted in Figure 3.4, seven (7) are influencing elements, while the ninth (9th) combines all elements to form a cybersecurity framework. The influencing elements in the proposed conceptual framework are I) ***Cybersecurity resources,*** II) ***Alignment of business and cybersecurity***, III) Practical and enforceable legislation, IV) Shared threat intelligence, V) Cybersecurity awareness, VI) Cybersecurity culture, and VII) ***Understanding cybersecurity***. All seven elements feed into the oval in the centre of Figure 3.4, converging to contribute to a cybersecurity framework. This is the final theoretical framework informed by findings in the literature, qualitative data, and quantitative data.

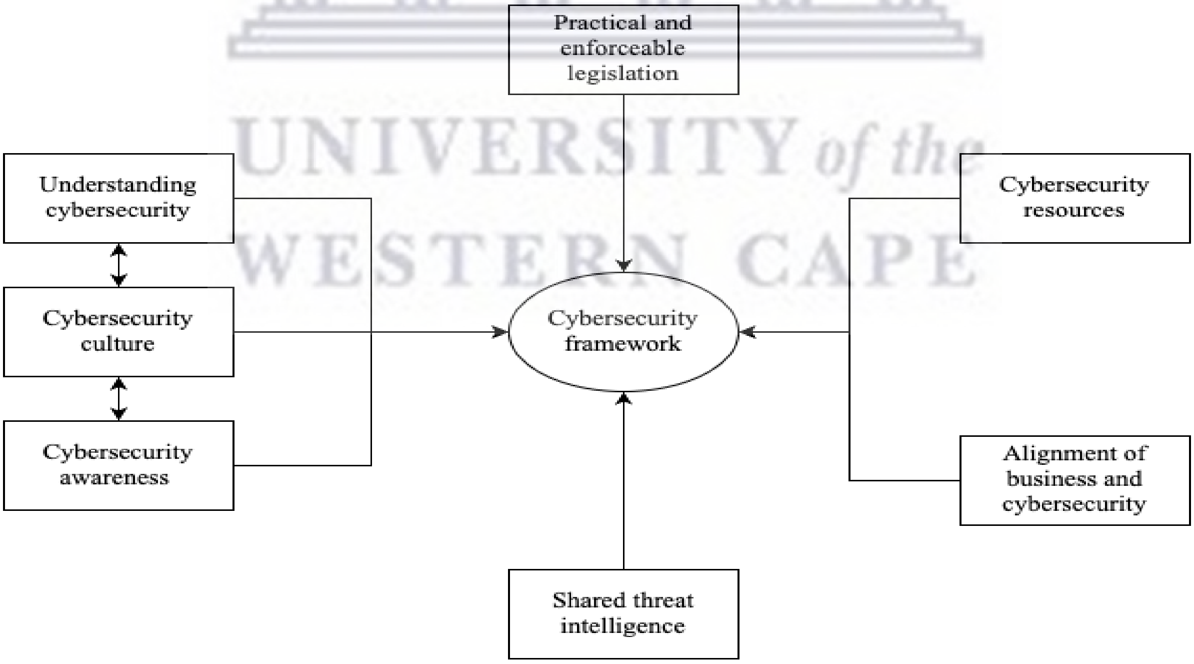

Practical and enforceable legislation
Understanding cybersecurity
Cybersecurity resources
Cybersecurity culture
Cybersecurity framework
Cybersecurity awareness
Alignment of business and cybersecurity
Shared threat intelligence

Figure 3.4 Conceptual Cybersecurity Framework: (Author, 2023)

The converged factors continuously interact with each other, thereby forming complex and non-linear relationships that work to establish a cybersecurity framework that addresses security from a people, processes and technology approach that, given the complexity of the interplay between the factors and the inherent nature of cybersecurity is a complex problem that continuously strikes a balance between security and business requirements.

It was impossible to propose a linear conceptual framework to address cybersecurity from one perspective. For this reason, the study employed theoretical frameworks that account for chaos and unpredictable contributors to systems.

Given the proposed conceptual framework, if any approach to address cybersecurity within commercial banks does not utilise a three-pronged approach that addresses people, processes, and technology, it becomes challenging to address cybersecurity challenges adequately in commercial banks.

Parent and Cusack (2016) posited that cybersecurity requires alchemy between technologies, people and processes, with the processes including regulations and laws.

3.4.1 Elements Of The Proposed Conceptual Model

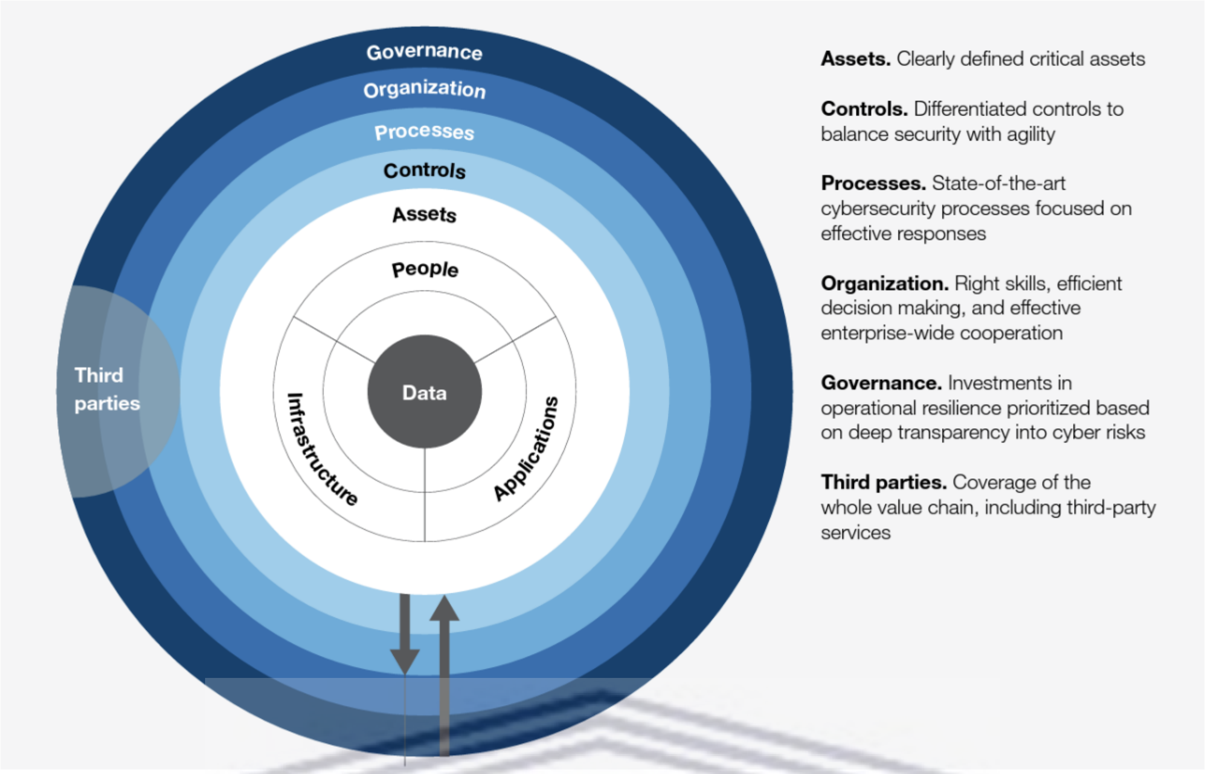
The seven elements mentioned above comprise the conceptual model and are discussed further below.

I. **Cybersecurity resources**

Organisations need sufficient resources to tap into to defend against cybercrimes and threats adequately. Regarding this factor as part of the conceptual framework, the researcher decided to group multiple themes that form part of cybersecurity resources. This is because no single resource would be enough to address the cybersecurity challenge.

Boehm, Merrath, Poppensieker, Riemenschnitter and Stähle (2018) stated that a holistic approach to cybersecurity may be used to address the cybersecurity problem within organisations because a holistic approach enables organisations to get an accurate overview of the risk landscape and further empowers them to focus their defences on the most likely and most threatening cyber risk scenarios.

Figure 3.5 briefly overviews the resources needed in a holistic approach to cybersecurity.



Assets. Clearly defined critical assets

Controls. Differentiated controls to balance security with agility

Processes. State-of-the-art cybersecurity processes focused on effective responses

Organization. Right skills, efficient decision making, and effective enterprise-wide cooperation

Governance. Investments in operational resilience prioritized based on deep transparency into cyber risks

Third parties. Coverage of the whole value chain, including third-party services

Figure 3.5 Resources in holistic cybersecurity approach. Source (Boehm, Merrath, Poppensieker, Riemenschnitter, & Stähle, 2018)

Teichmann (2020) supported this notion by stating that a cybersecurity approach needs to address people, skills, technology, processes, and governance. Adopting such an approach opens the door to cybersecurity resilience, which moves the focus away from keeping hackers out of business and more towards enabling businesses to continue operations as usual by minimising the damage and continuity risks posed by cyber-attacks.

- **Skilled cybersecurity personnel**

A shortage of cybersecurity skills is a global phenomenon that has steadily increased, along with the increasing number of cyber-attacks and threats in recent times. In a report published by the (ISC)^2 (2023)' they estimated that to protect cross-industrial enterprises from the increasingly complex and sophisticated modern-day threat actors, a global skills gap of 3.4 million cybersecurity workers would need to be filled. Challenges with overcoming the skills shortage are that cybersecurity careers require a range of talents and skills, making recruiting and upskilling for those roles even more challenging (World Economic Forum, 2023). In a survey conducted by ITWeb (2022) concerning the cybersecurity skills shortage in South Africa, more than half of the participants stated that their organisations were experiencing a skills shortage that adversely affected their detection and response capabilities. Section 2.5.1 delves into greater detail concerning the skills shortage in South Africa.

- **Financial resources**

It is less expensive to prevent a cyber-attack than it is to repair the damage when it happens (Crawley, 2020). Joyce (2020) proposed that a cyber strategy that considers cybersecurity in every business decision means connecting cyber budgets to organisational budgets in a risk-aligned and data-driven way. By doing so, organisations can quantify the overall value of cyber investments against business objectives.

- **Tooling**

Tooling is integral to getting visibility into the organisation's activities and mitigating threat actors. Various tools provide visibility and protection to different aspects of an organisation. Adequate investment in tooling is necessary to enable security teams' appropriate detection, response, and remediation efforts.

CheckPoint (2022) stated that the tools required by organisations fall into the following categories: Network Security, Cloud Security, Endpoint Security, Mobile Security, IoT Security, Application Security, and Zero Trust. Thompson (2020) further stated that some of the tools required by organisations are not physical but instead are operational teams that utilise the tools acquired by the organisation.

II. **Alignment of business and security**

Striking a balance between usability and security is key to getting the best value out of security without hampering the businesses. Jarjoui and Murimi (2021) stated that aligning IT and business involves a harmonious relationship between business objectives and IT. It is vital in coordinating and streamlining organisational efforts to combat cyber risks.

To achieve alignment, Blum (2020) stated that business leaders and organisational staff needed to see cybersecurity as a strategic programme and should perceive the security team as a business partner instead of merely a blocker.

By adopting such a view, security staff could rely on businesses to enable them to perform security-related duties. Simultaneously, owners who are threatened by business risks could be coached to make better risk-driven decisions. Figure 3.6 depicts how a CISO leads the security team to engage and align with the business at all organisational levels.

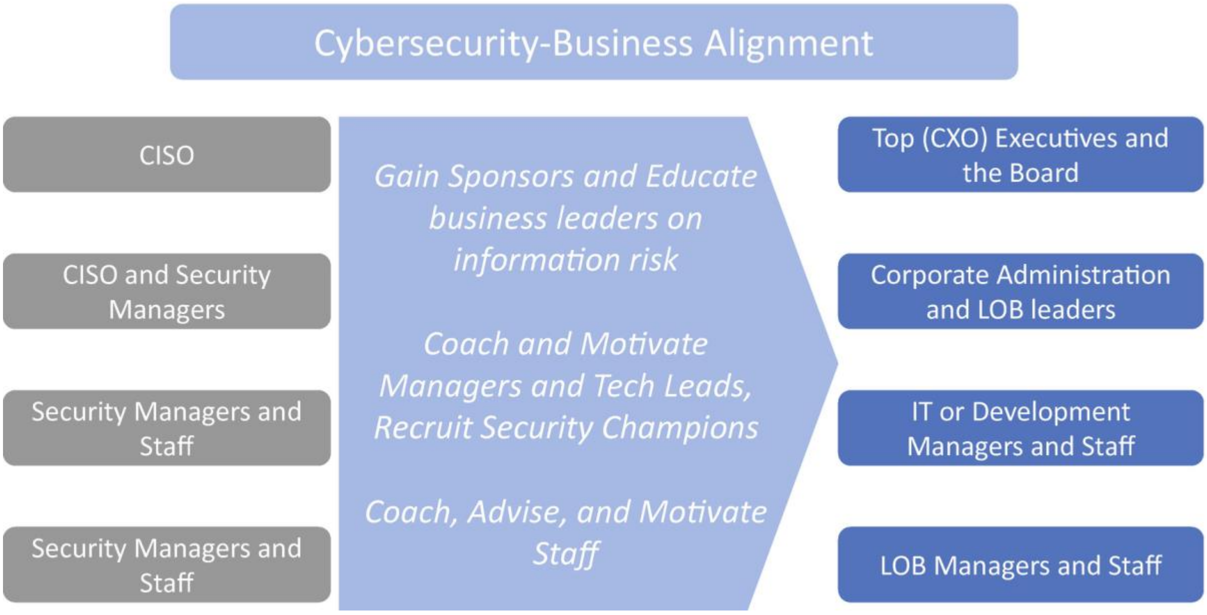

Cybersecurity-Business Alignment
CISO
CISO and Security Managers
Security Managers and Staff
Security Managers and Staff
Gain Sponsors and Educate business leaders on information risk
Coach and Motivate Managers and Tech Leads, Recruit Security Champions
Coach, Advise, and Motivate Staff
Top (CXO) Executives and the Board
Corporate Administration and LOB leaders
IT or Development Managers and Staff
LOB Managers and Staff

Figure 3.6 Cybersecurity-business alignment stack; Source Blum (2020)

Srinidhi, Yan, and Tayi (2015) posited that an optimal model enables adequate resource allocation to revenue generation while improving security activities simultaneously. However, misalignment in the form of excess insurance coverage may result in a moral hazard where resource allocation to security is reduced due to excessive cover. This would harm an organisation's ability to defend itself adequately against cyber threats. Therefore, a delicate balance must be achieved, resulting in adequate resourcing for security and ensuring the business meets its objectives.

III. Practical and enforceable legislation

Legislation regarding cybersecurity in the country in recent times has been chiefly centred around the Cybercrimes Act 19 of 2020, the Protection of Personal Information Act 4 of 2013 and the NCPF passed by Cabinet in 2012, which was an attempt to bring a level of coherence and coordination to the previous incoherent and fragmented pieces of legislation within South Africa; when addressing cybersecurity and information security. Although these regulations and laws have brought a sense of coherence to addressing cybersecurity in the country, Bote (2019) stated that the NCPF excelled at bringing together a myriad of theoretical viewpoints to address a rapidly changing problem, which, in turn, leads to a policy framework that does not provide a practical approach to dealing with the issue. The framework takes a liberalist view in emphasising the importance of cooperation and economic security but does not provide stakeholders with a realistic way of achieving that. Sutherland (2017) further stated that the NCPF appears to have been drafted without considering its implementation. This is further supported by the fact that since its adoption by the Cabinet, the NCPF has not been updated to deal with the rapidly changing cybersecurity threat landscape.

The researcher believes that although the government has made advances in adopting legislation that intends to protect the cyberspace of the country and the citizens' rights, a lot must be done regarding fully implementing the initiatives set out in the adopted legislation. Some aspects of the Cybercrimes Act and the NCPF are impractical. The Cybercrimes Act requires financial institutions and electronic communications service providers (ECSP) to report all offences to the SAPS within 72 hours. However, the odds of the SAPS having adequately skilled personnel to deal with the issue are slim, given the country’s shortage of IT skills (Tredger, 2023; Von Solms, 2022). Dlamini and Mbambo (2019) stated that considerable efforts are needed to upskill police officials with cybersecurity skills concerning prevention, investigation, prosecution/adjudication, and sentencing.

IV. Shared threat intelligence

The banking sector forms part of the country’s critical infrastructure, and, as such, its defence should be a consolidated effort between all stakeholders, including the government. However, challenges exist concerning the government. Mutemwa, Mtsweni and Mkhonto (2017) stated that the various arms of the defence force in the country operate in silos, which introduced challenges such as an imbalance of capabilities, limited security, and protection of critical infrastructure.

ENISA states that information sharing and analysis centres provide a central resource for gathering information on cyber threats and enable bilateral sharing of information between the private and public sectors about root causes, incidents, threats, experiences, knowledge, and analysis (European Union Agency for Network and Information Security (ENISA), 2017).

SABRIC is a non-profit company formed by the banking industry of South Africa to assist its members with creating, maintaining, and supporting viable and sustainable banking, as well as having financial crime combating capabilities to enter into beneficial collaborative partnerships to achieve its strategic objectives, to contribute to national crime combating priorities and to contribute to the general safety, security and cyber resilience within the banking domain, for the benefit of the South African public (SABRIC, 2023).

The International Monetary Fund (IMF) (2022) stated that the process for combating cyber incidents in South Africa was cumbersome and that there was a need to implement an industry-wide platform to facilitate cyber threat intelligence sharing. Furthermore, they said that, given the SARB's capabilities and centrality in the financial sector, there should be greater emphasis on improving information sharing and community building in the Community of African Banking Supervisors (CABS). Internally, banks must foster a culture of information sharing and transparency between their departments and stakeholders. Chigada and Ngulube (2015) identified siloed cultures in banks as an impediment to information sharing.

V. Cybersecurity awareness

Venter, Blignaut, Renaud and Venter (2019) posited that cybersecurity education has two elements: firstly, there is a need for people to become aware that they need to take precautions online, and secondly, for teachers, there is a need to impart skills that are required to implement cautious behaviour online. Cybersecurity awareness for this study was extended to include human behaviour, precisely end-user behaviour for those employed within the banks and for customers using the digital services made available by banks. Chigada (2020) stated that unacceptable human behaviour is at the forefront of cyber-attacks, threats, and information system security.

This view is supported by multiple scholarly opinions, considering humans the weakest link in the proverbial cybersecurity chain. Li *et al*. (2019) posited that users were the weakest link in cybersecurity because some did not pay attention to organisational security policies, while others tended to underestimate security risks. However, they were aware of institutional security policies.

Addressing cybersecurity awareness first starts with acknowledging the issue because cybersecurity threats and cybersecurity awareness should be associated with positivity, meaning that the more aware an individual is, the more unlikely they are to engage in risky behaviour online (Lee & Kim, 2022). The South African government responded to increasing cybersecurity awareness by passing the NCPF in March 2012. The hub was established by the Department of Telecommunications and Postal Services in 2015 to provide information that created awareness of cybersecurity that would encourage South African citizens and organisations to be secure online (Department of Telecommunications and Postal Services, n.d.). One of the initiatives launched by the hub was Qaphela I Online™, which aimed to provide resources for individuals and organisations regarding online security. Although the establishment of a national institution to drive cybersecurity awareness is a positive thing, Rama and Keevy (2022) argued that in comparison to the USA, UK, Saudi Arabia, and Estonia, South Africa still has substantial room to improve because firstly, the NCPF which mandated for the establishment of the cybersecurity hub has not been updated since 2015. Secondly, better cooperation between the government, the private sector, international parties and society is still lagging behind other countries regarding cybersecurity awareness. Thirdly, education around cybersecurity awareness can be improved by making training programmes more accessible to the public.

VI. Cybersecurity culture

Definitions of cybersecurity culture, information security culture and security culture are often intertwined. Still, most of the definitions stem from Dhillon's (1997) paper that described security culture as the 'totality of human attributes such as behaviours, attitudes and values that contribute to the protection of all kinds of information in a given organisation' and from Martins and Eloff's (2002) definition which posited security culture as an 'assumption about perceptions and attitudes that are accepted to incorporate information security characteristics as to how things are done in an organisation'; both of which supported the notion that human behaviour and attitudes contribute to the information security culture. Chigada (2021) stated that the cybersecurity culture remains an ill-defined problem that lacks accepted key concepts that delimit it.

Uchendu *et al.* (2021) noted the key factors influencing internal cybersecurity culture in organisations: support and leadership from top management, clear policies and governing procedures for employees to follow, security awareness and training, and change management. Da Veiga *et al.* (2020) further supported their views by stating that the internal factors influencing cybersecurity culture are organisational, management, human, and mutual trust. Additionally, the NCPF calls for establishing a strong cybersecurity culture within the country. It tasks civil society, government and private security with driving cybersecurity awareness and fostering a positive narrative regarding cybersecurity within the republic (Republic of South Africa, 2015).

Stackpole (2022) stated that embedding safety into the fabric of every employee ensures that they are constantly reminded of their role and responsibilities and establishes a strong cybersecurity culture in organisations. Furthermore, reinforcing culture may be driven from three levels: i) the leadership level, ii) the group level, and iii) the individual level.

VII. **Understanding cybersecurity**

Chigada (2021) stated that various contributors' beliefs could be attributed to the lack of understanding of cybersecurity, such as the lack of information and knowledge sharing platforms. One key contributor may be the lack of a clear and industry-wide definition of cybersecurity. Multiple definitions of cybersecurity add to the complexity when one is trying to understand a problem because cybersecurity and information security are often used interchangeably, which should not be the case, given that each element addresses specific issues regarding security. Von Solms and van Niekerk (2013) stated that information security protects information as an asset used to protect individuals from possible harm from threats and vulnerabilities. Conversely, cybersecurity is defined 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 an organisation's and user's assets (The International Telecommunications Union, 2017).

Within the South African context, this lack of understanding may also be attributed to a rigid national learning structure that does not make it possible for students to undertake multidisciplinary studies, which are often required when tackling cybersecurity due to its diverse nature. Furthermore, the school curriculum in South Africa does not provide an adequate foundation in STEM fields, which is a prerequisite for those desiring to pursue cybersecurity in the future (Ramluckan *et al.*, 2020). The South African government's delayed adoption of POPIA and the Cybercrimes Act may also indicate a lack of understanding of cybersecurity. This is so because other nations across the globe had already proposed and accepted legislation concerning cybersecurity long before the South African government recognised the problem.

3.5 Chapter Summary

This chapter introduced and discussed the theoretical frameworks that guided the study. The frameworks covered included well-established frameworks such as complexity theory, chaos theory, systems theory and a lesser-known but essential framework when addressing cybersecurity within South Africa, the NCPF. The chapter discussed how these frameworks contributed to the lens through which the study was conducted, which presented those frameworks within the cybersecurity domain. The chapter also introduced the proposed conceptual framework for commercial banks. The framework comprised seven factors that interplay and influence each other. The seven factors converged into a singular oval shape representing the proposed framework. The next chapter builds on this chapter by detailing the research design and methodologies employed in the study. It considers the possible research designs that could have been used for the study, contrasts them with the chosen option, and then expounds on the selected research design and the adopted philosophical paradigm.

PART III

Chapter Four : Research Design And Methodology

4.1 Introduction

This chapter outlines the research design and methodology adopted for the study. Leedy (2010) defined research as a systematic process of collecting, analysing, and interpreting data to increase our understanding of a phenomenon that a researcher is interested in or concerned about. Formal research aims to enhance our understanding of a phenomenon and then communicates what the researcher has discovered to the larger scientific community.

The research methodology is a researcher's general approach when conducting a research project (Leedy & Ormond, 2016). Research can be compared to the layers of an onion (Figure 4.1), with each layer representing an aspect of the research and the centre being the data collection and analysis phase. Each layer of the onion (an element of research) will be considered in this chapter.

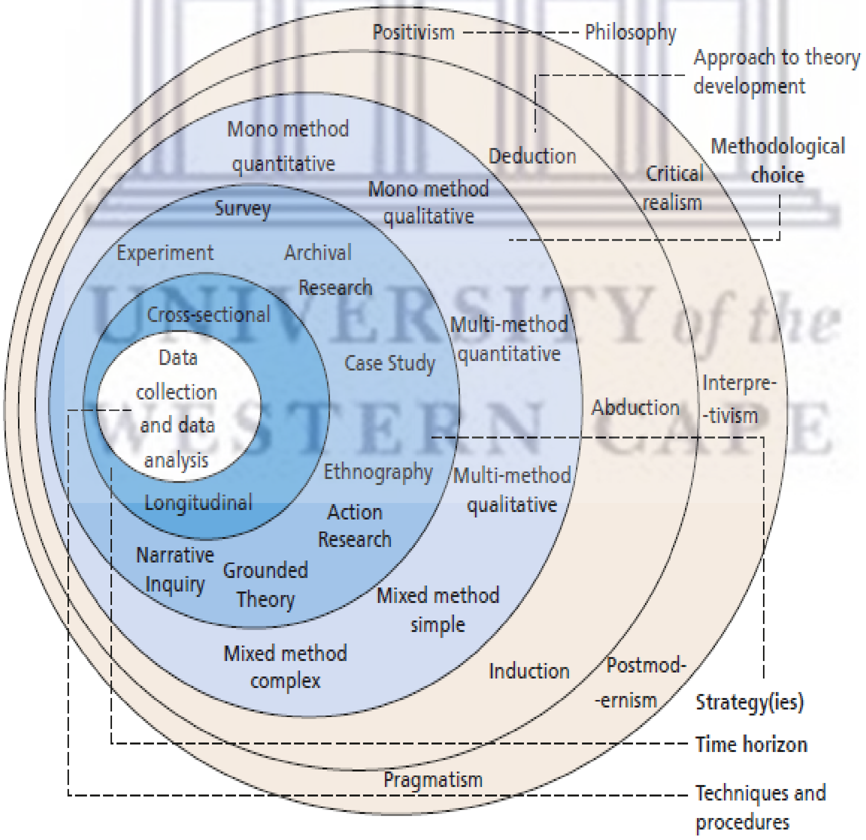


Figure 4.1 The research onion. Source: (Saunders, Lewis, & Thornhill, 2019)

4.2 Research Paradigm/Philosophy

A paradigm is a set of assumptions and perceptual orientations of research community members (Given, 2008). Saunders *et al.* (2019) further stated that a paradigm is a set of basic assumptions that are taken for granted, which underwrite the frame of reference, mode of theorising and ways of working in which a group of researchers operates. These assumptions determine how members of a research community view the phenomena in their particular community and the research methods that should be employed to study those phenomena (Given, 2008). Creswell and Plano Clark (2011) stated that all research had a philosophical foundation that shaped the research process and the conduct of inquiry. Multiple research philosophies and paradigms can be applied to studies. These include but are not limited to positivism, critical realism, interpretivism, and pragmatism.

Three research assumptions can be employed to distinguish research philosophies: ontology, axiology, and epistemology (Saunders *et al.*, 2019).

Ontology refers to the nature of reality (and what is real) that researchers assume when they conduct their inquiries (Creswell & Plano Clark, 2017). Jupp (2006) defined it as a concept concerned with the existence and relationship between different aspects of society, such as social actors, cultural norms, and social structures. **Axiology** considers the nature of value and what kinds of things have value (Littlejohn & Foss, 2009). It refers to the roles of values and ethics within the research process (Saunders *et al.*, 2019). **Epistemology** is concerned with the nature, sources, limits of knowledge and assumptions about knowledge – how we know what we say we know, what constitutes acceptable, valid, and legitimate knowledge, and how we can communicate knowledge to our fellow human beings (Saunders *et al.*, 2019; Mathison, 2005).

The following sections explore the different philosophies and paradigms, their epistemological, ontological, and axiological orientations, and offer brief overviews of the typical research methods.

4.2.1 Positivism

Positivism relates to the philosophical stance of the natural scientist and entails working with an observable social reality to produce law-like generalisations (Saunders *et al.*, 2019). Leedy and Ormond (2016) posited that positivism is a philosophical perspective based on the idea that scientists can objectively uncover absolute facts about cause-and-effect relationships in the physical world and human experience with appropriate techniques. Saunders *et al. (2019) further stated that positivism refers to the importance of what is "posited",* i.e., 'given'. This emphasises the positivist focus on the strictly scientific empiricist method to yield pure data and facts uninfluenced by human interpretation or bias. Positivism, however, does have its critics, with Alvesson and Sköldberg (2017) stating that its attendant reductionist posture with its focus on objective reality excludes an empathic understanding of social phenomena from an individual point of view. The other challenge researchers face when adopting positivism is adopting a value-free perspective, excluding their values when conducting research.

4.2.2 Critical Realism

Critical realism is a postpositivist philosophy that asserts that reality exists independently of our perceptions and that the underlying entities may not be directly observable or measurable. It also holds that our theories about reality depend on our beliefs and knowledge, both of which are fallible (Donald & Williams, 2020). It can further be defined as a theoretical or philosophical position that integrates a realist ontology (there is a real-world that exists independently of our perceptions, theories, and constructions) with a constructivist epistemology (our understanding of this world is inevitably a construction from our perspectives and standpoint) (Creswell & Plano Clark, 2017). Saunders *et al.* (2019) define critical realism as explaining what we see and experience regarding the underlying structures of reality that shape the observable events. Critical realism is also often seen as a middle way between empiricism/positivism on the one hand and anti-naturalism/interpretivism on the other, thus introducing a more nuanced version of realist ontology (Zachariadis, Scott, & Barrett, 2013).

4.2.3 Interpretivism

Interpretivism is a philosophy that emphasises that humans are different from physical phenomena because they create meaning (Saunders *et al.*, 2019). Introna, Kavanagh, Kelly, Orlikowski, and Scott (2016) defined interpretivism as a research avenue which sees knowledge of reality as a social construction and states that value-free data cannot be obtained. It starkly contrasts positivist studies, where objective data can be used to present a prior hypothesis.

4.2.4 Pragmatism

The pragmatic paradigm refers to a worldview that focuses on “what works” rather than what might be considered absolutely and objectively “true” or “real” (Frey, 2018). Instead, it accepts that there can be single or multiple realities open to empirical inquiry (Creswell & Plano Clark, 2011). It may be defined as a philosophical perspective based on the idea that absolute truth about certain phenomena and people’s constructed beliefs about them are legitimate objects of study. It is also known as realism (Leedy & Ormond, 2016).

4.3 Research Philosophy/Paradigm Choice

According to Frey (2018), the choice of a paradigm is influenced by sets of elements unique to each that define its assumptions of ontology, epistemology, axiology, and methodology. The study employed a pragmatic research philosophy that is not committed to any single system of philosophy (epistemology) or reality (ontology). This ontological and epistemological stance made it possible to combine multiple data collection techniques and methods within the study to improve the reliability and validity of the research findings.

Pragmatism embraces the idea that philosophy does not occur before science but continues with it (naturalism). It uses science but is also open to exploring different methods employed in other branches of science (Frey, 2018). In pragmatism, the approach taken by a researcher may combine deductive and inductive thinking, as the researcher mixes both qualitative and quantitative data as they conduct the study (Creswell & Plano Clark, 2011). This is because pragmatism allows researchers to be flexible in their investigative techniques as they attempt to address a range of research questions that arise therefrom (Onwuegbuzie & Leech, 2005). Pragmatism also enables researchers to use qualitative research to inform the quantitative portion of research studies and vice versa (Onwuegbuzie & Leech, 2005). Madey (1982) stated that combining qualitative and quantitative research helps the researcher develop a conceptual framework, validate quantitative findings by referring to information extracted from the study’s qualitative phase, and then construct indices from the qualitative data that can be used to analyse the quantitative data.

The focus is on the consequences of research, the primary importance of the question asked rather than the methods used, and multiple data collection methods to inform the problem under study (Creswell & Plano Clark, 2017)

4.4 Research Design

Research design provides the overall structure for the procedures a researcher follows, the data the researcher collects, and the data analysis the researcher conducts afterwards (Leedy & Ormond, 2016). Lavrakas (2008) defined research design as a general plan or strategy for conducting a research study to examine specific testable research questions of interest. De Vaus (2001) posited that the function of a research design is to ensure that the evidence obtained enables us to answer the initial question (research question) as unambiguously as possible. Rassel, Leland, Mohr and O'Sullivan (2020) offered specific and general definitions of research design. In light of the preceding choices, the researcher can then decide on the type of methodology and study they wish to conduct.

Research can be designed to fulfil an exploratory, descriptive, explanatory, or evaluative purpose (Saunders *et al.*, 2019). An overview of these research designs is given below:

- **Exploratory** studies are a valuable means to ask open questions to discover what is happening and to gain insight into a topic of interest (Saunders *et al.*, 2019). They typically begin with and prioritise data collection and analysis of qualitative data and build from the exploratory results; the researcher then conducts a development phase by designing a quantitative feature based on the qualitative results (Creswell & Plano Clark, 2017). Exploratory studies are usually used when studying a new or relatively under-researched topic. They help fill in knowledge gaps or offer different perspectives on phenomena to generate new and emerging insights (Leavy, 2017).
- **Descriptive** designs are intended to describe people, products, or situations. They usually have one or more guiding research questions but are generally not driven by a structured research hypothesis (Sue & Ritter, 2012). They aim to gain a profile of events, persons, or situations. This design made it possible to draw a profile of cybersecurity within commercial banks in South Africa by collecting data from employees and reports of cybersecurity incidents that had taken place in recent times.
- **Explanatory** designs have the primary purpose of explaining why phenomena occur and predicting future occurrences. They are characterised by research hypotheses that specify the nature and direction of the relationship between or among the variables being studied (Sue & Ritter, 2012). They are most effective in establishing a causal relationship or a correlation between variables. Thus, they cannot effectively be applied to studies where relationships between variables might not exist (Saunders *et al.*, 2019).

- **Evaluative** designs mainly focus on determining the effectiveness of programmes or materials and less on understanding why those programmes or materials may or may not be effective (Reinking & Alvermann, 2005). They are undertaken to assess the worth or success of something, such as a programme, a policy, or a project (Payne & Payne, 2004). This type of design is concerned with how something works or the effectiveness of the subject under study. The questions asked during data collection seek an evaluative understanding of the subject and might also make comparisons between events, situations, groups, places, or periods (Saunders *et al.*, 2019). Evaluative designs do not fit this study as usually the result of such a study is a theoretical contribution emphasising understanding 'how effective' something is and 'why.'

Each design follows particular research strategies, with a research strategy being a plan of how a researcher will answer their research question (Saunders *et al.*, 2019). It is a methodological link between the research philosophy and the subsequent choice of methods to collect and analyse data (Denzin & Lincoln (2018) (cited in *Saunders et al.*, 2019). Common research strategies are mentioned below:

- **Experimental**: An experimental design aims to study the probability of change in an independent variable which causes a change in another dependent variable. It uses hypothetical explanations, known as hypotheses, rather than research questions (Saunders *et al.*, 2019).
- **Cross-sectional**: Bryman (2012) defines cross-sectional design as a research design that entails the collection of data on more than one case (usually quite a lot more than one) and at a single moment in time, to collect a body of quantitative or quantifiable data in connection with two or more variables (usually more than two), which are then examined to detect patterns of association.
- **Longitudinal**: This research design involves repeated measurement over time of one or more groups of subjects (Deschenes, 1990). Leedy and Ormond (2016) define longitudinal design as a research design where a single group of people are followed over several months or years, and data related to the characteristic(s) under investigation are collected at various times.
- **Case study**: This research strategy concerns the complexity and particular nature of the case in question, Stake (1995) (cited in Bryman, 2012). A specific individual, programme, or event is studied in-depth for a defined period (Leedy & Ormond, 2016).

Yin (2018) stated that case studies allow one to focus in-depth on a case and retain a holistic and real-world perspective.

- **Comparative**: Comparative design entails studying two contrasting cases using more or less identical methods. It embodies the logic of comparison, implying that we can understand social phenomena better when comparing two or more meaningfully contrasting cases or situations (Bryman, 2012).

4.5 The Chosen Research Design For This Thesis

The research strategy for the chosen study was descriptive design, which is usually characterised by research questions that begin with or include 'Who,' 'What,' 'Where,' 'When', or 'How' (Saunders *et al.,* 2019). Descriptive research examines a situation and does not involve changing or modifying the situation under investigation (Leedy & Ormond, 2016). This design made it possible to profile current perceptions and sentiments and to examine the overall cybersecurity landscape within commercial banks in South Africa through the eyes of employees who form a critical part of any cybersecurity framework. The design allowed for addressing the 'How' part of the leading research question using various data collection approaches. The research design was undertaken in two phases: Phase 1 – collecting considerable qualitative data through interviews, and a second phase - collecting quantitative data through surveys to follow-up on the first phase of data collection. By adopting these two phases, we could better understand the data collected from each phase and use the data to cross-validate the findings from each collection method.

4.6 Research Methodology

Rassel *et al.* (2020) defined research methodology as a structured set of steps and procedures for completing a research project. Saunders *et al.* (2019) posited research methodology as the theory of how research should be undertaken and research methods as the techniques or procedures used to obtain and analyse data. These could include surveys, observations, and interviews, as well as both quantitative (statistical) and qualitative (non-statistical) analysis techniques (Saunders *et al.*, 2019). There is a clear difference between research methods, which equate to research tools, and research methodology, which is more concerned about the general approach the researcher takes in carrying out a research project (Leedy & Ormond, 2016). Three research methodologies were considered for the study: qualitative, quantitative, and mixed research methods. A brief description of each of the methodologies is given below:

Qualitative research methods: Myers (2019) (cited in Iyamu, 2018) described qualitative research methods as methods that enable researchers to study phenomena in their natural settings, which is essential in the real world. They study participant’s meanings and their relationship, using various data collection techniques and analytical procedures to develop a conceptual framework and then offer a theoretical contribution (Saunders *et al.,* 2019). Malhotra, Nunan and Birks (2017) described the nature of qualitative research as one that encompasses a variety of methods that can be applied flexibly to allow participants to reflect upon and express their views or enable researchers to observe their behaviour.

Quantitative research methods: This method is usually associated with a deductive approach, where data is collected and analysed to test a theory. However, it may also incorporate an inductive approach, where data are used to develop theory Saunders *et al.,* 2019). O’Sullivan, Rassel, Berner, and DeVance Taliaferro (2017) defined quantitative research as research in which numbers and data characterise the values of variables, which are then summarised and analysed using statistical techniques. Quantitative studies comprise survey research, which involves acquiring information about one or more groups of people regarding their characteristics, opinions, attitudes, or previous experiences (Leedy & Ormond, 2016).

Mixed research methods: Mixed method designs are those that include at least one quantitative method (designed to collect numbers) and one qualitative method (designed to collect words), where neither type of method is inherently linked to any particular inquiry paradigm (Creswell & Plano Clark, 2017). The core of mixed methods, according to Creswell and Plano Clark (2011), is that the researcher:

- Collects and analyses both qualitative and quantitative data rigorously in response to research questions and hypotheses,
- Combines two forms of data and their results,
- Organises these procedures into specific research designs that provide the logic and procedures for conducting the study and,
- Frames the procedures within theory and philosophy.

4.6.1 Methodological Choice for This Thesis

The study employed mixed methods, providing a qualitative dimension that brought out cybersecurity's social and human aspects, followed by a quantitative approach. Tashakkori and Creswell (2007) defined mixed methods as research wherein the investigator collects and analyses data integrates the findings, and draws inferences using qualitative and quantitative approaches and methods in a single study or programme of inquiry. Using mixed methods allows researchers to address complex research questions, find answers to exploratory and confirmatory questions within a single study, and reveal a fuller picture of the problem in practice (Greene, 2007; Teddlie & Tashakkori, 2008).

Within mixed methods, there exist three core designs from which a researcher can choose: convergent, explanatory sequential, and exploratory sequential. The study used convergent parallel mixed methods, which Creswell (2011) defines as a method in which the researcher concurrently collects and analyses two separate databases (quantitative and qualitative) and then merges the two databases to compare the results or add transformed qualitative data as numeric variables into the quantitative database. The convergent approach assisted in obtaining different but complementary data on the same topic.

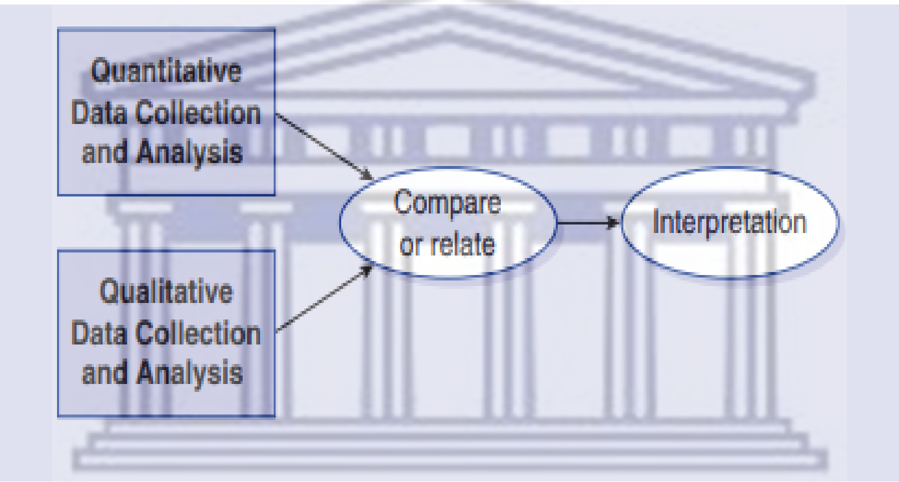

Quantitative Data Collection and Analysis
Qualitative Data Collection and Analysis
Compare or relate
Interpretation

Figure 4.2 Convergent parallel design. Source (Creswell & Plano Clark, 2017)

Mixed methods were used for the study because they provided a way to harness strengths that offset the weaknesses of both quantitative and qualitative research (Creswell & Plano Clark, 2017). They also offered more evidence for studying a research problem than quantitative or qualitative research alone (Creswell & Plano Clark, 2017).

Saunders *et al.* (2019) also stated that mixed methods allow for a greater diversity of views to inform and be reflected in a study that uses mixed methods. They further posited that mixed methods make it possible to have greater confidence in conclusions because the mixed methods have the potential to cancel out the shortcomings of one process.

Hesse-Biber (2010) stated that mixed methods enable a researcher to look for convergence of the data collected by all methods in a study to enhance the credibility of the research findings.

Mixed methods triangulation ultimately fortifies and enriches a study's conclusions, making them more acceptable to advocates of both qualitative and quantitative methods (Hesse-Biber, 2010).

4.7 Target Population

Concerning the research design and statistical analysis, a population is the entire collection of entities one seeks to understand more formally or to draw an inference from (Salkind, 2010). The target population defines the units the study findings are meant to generalise (Lavrakas, 2008). It comprises all the people or objects to which a study wishes to generalise its conclusions. Saunders *et al.* (2019) further defined it as the complete set of cases or group members that are the actual focus of the research inquiry and the method whereby a sample may be drawn.

The target population was employees from commercial banks in South Africa, with a significant focus on technical employees within the IT domain of the respective banks. This included but was not limited to individuals with positions such as software developers, network engineers, business analysts, system architects, IT engineers, security engineers, information security officers, risk analysts, cyber incident response personnel, privacy and governance personnel, technical managers, and team leaders. The table below (Table 4.1) depicts the number of employees some of the respective commercial banks employ and gives an overview of the population. This list is not exhaustive and only comprises large commercial banks in South Africa. The population of employees from commercial banks was far too large to consider for the entire study, so a sample population was selected.

Table 4.1 Number of employees

Commercial Bank	Number of Employees
A	3815[4]
B	14672[5]
C	27160[6]
D	28324[7]
E	39240[8]
F	47000[9]
Total Number of employees	160211

4.8 Sampling

Bryman (2012) defines a sample population as a segment of the selected population for research. It is a subset of the population, and this selection method may be based on probability sampling or nonprobability sampling principles.

There are two types of sampling strategies: namely, probability or representative sampling and nonprobability sampling. Probabilistic sampling is a technique where a researcher selects many individuals who represent the population or a segment of the population (Creswell & Plano Clark, 2017). Babbie (2010) further defined it as a technique whereby samples are selected using probability theory, and typically, it involves a random selection technique. Nonprobability sampling is any technique in which samples are chosen somehow but not by probability theory (Babbie, 2010). Within statistical sampling, bias exists, which Bruce & Bruce, 2017 defined as a measurement or sampling error that is systematic and is produced by the measurement or sampling process. Bias occurs when a sample is systematically not representative of the inference population in some way (Fricker, 2012).

Under probability sampling and nonprobability, there are a variety of strategies that can be applied to studies. Some of these strategies are:

- **Simple random sampling** – each member of the target population has an equal chance of being included in any given sample (Hesse-Biber, 2010). This type of sampling can

[4] African Bank Holdings Limited Consolidated Annual Financial Results September 2020

[5] From the 2021 Integrated annual report https://www.capitecbank.co.za/investor-relations/financial-results/2021/

[6] As of the 2020 annual results https://www.absa.africa/absaafrica/investor-relations/financial-results/

[7] As of 2020 annual results https://www.nedbank.co.za/content/nedbank/desktop/gt/en/investor-relations/information-hub/financial-results/2020.html

[8] From the December 2020 interim results https://www.firstrand.co.za/investors/financial-results/

[9] The number of employees includes those in South Africa and Africa regions. Source is the 2020 SBG Report to Society https://reporting.standardbank.com/results-reports/annual-reports/

be performed with replacement or without replacement. With replacement, observations are put back into the population after each draw for possible future reselection. Conversely, each selected observation is not returned to the population without replacement, making it unavailable for future selection (Bruce & Bruce, 2017). This sampling method is intended to be unbiased, as each member has an equal chance of being selected.

The probability of a member being selected without replacement is:

$$P = \frac{N-n}{N-(n-1)}$$

Equation 4.1 Simple random sampling without replacement

Where *N* is the known population size, and *n* is the known sample size

The probability of a member being selected with replacement:

$$P = 1-\left(1-\frac{1}{N}\right)^{n}$$

Equation 4.2 Simple random sampling with replacement

N is the known population size, and *n* is the sample size.

- **Stratified random sampling** – the researcher divides the target population into desired groups for sampling. Then, they randomly select population elements within each group until the target sample size is reached (Hesse-Biber, 2010). The population elements are divided into distinct groups (strata), where within each stratum, the elements are similar concerning selected characteristics of importance to the survey. Then, typically, each stratum is independently sampled using a method for which an unbiased estimator of the stratum mean can be computed (Parsons, 2017). This sampling method is typically used in sample surveys as it increases the efficiency of sample design concerning cost and population estimator precision.
- **Cluster sampling** – in cluster sampling, all the population elements are categorised into mutually exclusive and exhaustive groups called clusters. The clusters are selected for sampling, and all or some elements from selected clusters comprise the sample (Frey, Cluster Sampling, 2018). Clustering may include single or multiple stages of clustering known as multistage and single-stage cluster sampling or one-stage cluster sampling (Levy, 2014). Multistage sampling involves an initial selection based on groups of elements in the population, referred to as primary sampling units. A second-stage sample follows, drawing a subsample from each selected primary sampling unit.

By repeating the process, higher sampling stages occur (SAS Institute Inc., 2013) while only operating once, resulting in a single-stage or one-stage cluster. This form of sampling is best suited for sampling units (elements) over prominent geographic locations, as it saves time and money.

- **Systematic random sampling** – A type of probability sampling in which every k^{th} unit in a list is selected for inclusion in the sample (Babbie, 2010). It involves selecting the sample at regular intervals from the sample frame (Saunders *et al.,* 2019). The sampling interval is determined by dividing the population size *N* by the sample size *n* and rounding to the nearest whole number. As with simple random sampling, each population element has a known and equal probability of selection. However, it differs from simple random sampling in that only the permissible samples of size *n* that can be drawn have a known and equal probability of selection (Malhotra *et al.*, 2017). It assumes that the population elements are ordered in some respect because if they are unordered in some instances, they produce comparable results to simple random sampling. If they are ordered concerning some characteristic, it increases the sample's representativeness (Malhotra *et al.*, 2017).
- **Nonprobability convenience sampling** –the research question determines the elements selected (Hesse-Biber, 2010). It attempts to obtain a sample from convenient elements, with the selection of elements often left up to the researcher. It is, however, prone to bias, as it is not representative of the population, and the analysis of results can only be applied to selected sample elements (Malhotra *et al.,* 2017; Stratton, 2021).
- **Purposive (judgemental) sampling** – is a nonprobability sampling method in which the units to be observed are selected based on the researcher's judgement about which ones will be the most useful or representative (Babbie, 2010). The purpose is to produce a sample that can logically be assumed to be representative of the population by applying expert knowledge of the population to select sample elements that represent a cross-section of the population (Lavrakas, Research Design, 2008).
- **Snowball sampling** – is a nonprobability sampling method often employed in field research, whereby each person interviewed may be asked to suggest additional people for interviewing (Babbie, The Practice of Social Research, 2010). It usually starts with a few initial contacts who fit the selection criteria. The participants are then asked to recommend other contacts who might contribute to the research. It requires the researcher to use their social networks to establish initial links with sampling

momentum developing from these links; sampling usually finishes when the target sample size has been reached or when a saturation point has been reached (Parker, Scott, & Geddes, 2019). Saturation in qualitative research is commonly taken to indicate that, based on the data collected or analysed hitherto, further data collection and analysis are unnecessary (Saunders *et al.*, 2018).

4.9 Sampling Strategy Of Choice

The sampling strategy employed for the study was snowball sampling. Snowball sampling is a nonprobability sampling method often employed in field research, whereby each person may be asked to suggest additional people for interviewing (Babbie, 2010). Using snowball sampling, the first set of individuals to participate in the study is used to reach a more significant population of participants from different commercial banks in South Africa. More details about individuals and reports relevant to the study were revealed through referrals from the first set of participants in the study. Eventually, as a cascading effect of this strategy, a comprehensive list of people and material in the cybersecurity domain of commercial banks was discovered and included in the study.

Snowball sampling is an effective method for initially exploring phenomena and populations for which few parameters are available to plan more formalised sample designs (Johnson, 2014). One of the significant advantages of snowball sampling, which is part of nonprobability sampling, is that it is quicker, easier, and usually cheaper than probability sampling (O’Sullivan *et al.*, 2017). This approach will also make it possible to overcome the challenges posed by the POPIA, under which employers (commercial banks in South Africa) cannot give out details about their employees without their explicit consent (Republic of South Africa, 2013).

4.10 Sample Size

Sample size usually refers to the number of units chosen from the gathered data (Lavrakas, 2008). When using sample size, one should consider sampling bias, which O’Sullivan *et al.* (2017) defined as a systematic misrepresentation of the population by the sample.

$$\text{Sample size} = \frac{\frac{z^2 \times p\,(1-p)}{e^2}}{1 + \left(\frac{z^2 \times p\,(1-p)}{e^2 N}\right)}$$

Equation 4.3 Sample Size Equation

N = population size

e = margin of error

z^2 = z-score

p = population proportion

$$sample\ size = \frac{\frac{1.96^2 \times 0.5\ \times (1-0.5)}{0.05^2}}{1 + \frac{1.96^2 \times\ 0.5\ \times (1-0.5)}{0.05^2 \times 160211}}$$

$$sample\ size =\ 383.24$$

$$sample\ size \sim 384$$

Using the formula above with a margin of error of 5 per cent, a confidence level of 95 per cent, and a population proportion of 50 per cent, 160211 is the total number of employees in commercial banks in South Africa. The sample size for the study was determined to be 384. To accommodate the likelihood of respondents not returning the survey or not completing the interviews, an additional 15 per cent of the sample population was added, bringing the total sample size to 442. From that sample size, the number of interviewees was determined to be twenty-one because Creswell and Plano Clark (2006) stated that identifying small numbers of people or sites in qualitative research provides in-depth information about each person or site. Conversely, the larger the number of people, the less detail typically emerges (Creswell & Plano Clark, 2006). The survey's sample size was the remainder of the entire sample population, 424.

4.11 Data Collection

The basic idea of data collection in any research study is to gather information to address the questions being asked in the study (Creswell & Plano Clark, 2011). Data collection is the process of collecting and measuring information on variables of interest in an established systematic fashion, which enables one to answer stated research questions, test hypotheses, and evaluate outcomes (Krishnamurthi, Cabera, & Karlovsky (2003) (cited in Stellenbosch University, 2021). It consists of multiple interconnected steps: sampling, gaining permission and recruiting participants, identifying data sources, recording the data, and administering the data collection procedures (Creswell & Plano Clark, 2011). Teddlie and Yu (2007) stated that data collection in a mixed methods study aims to develop answers to research questions. Multiple data collection methods exist and can be utilised by researchers. These methods usually fall into qualitative or quantitative methods, including interviews, semi-structured interviews, and surveys. Three data collection methods were employed: surveys, semi-structured interviews, and analysis of public reports concerning cybersecurity within commercial banks in South Africa.

The steps outlined by Morse, Barret, Mayan, Olson, and Spiers (2002) were followed to ensure the reliability of the data. The five steps aimed at methodological coherence to ensure congruence between the research questions are selecting the appropriate sampling groups, collecting and analysing data concurrently to understand what is known and what needs to be known, and then applying theoretical frameworks to develop a theory from the data.

4.11.1 Survey Structure

The survey was a custom survey centred around the objectives and research questions of the study. It had not been used in the field before, so it had to be piloted to collect input and feedback from potential respondents. The survey comprised three sections: Introduction, which comprised information about the researcher, the study being carried out, the information sheet, and informed consent. Before the respondents could proceed with the rest of the survey, they had to read the information sheet and agree to consent. Demographic information: the next section collected data about the respondents, such as their ethnic backgrounds, qualifications, the commercial bank they were employed by, and the job title they held.

The question section of the survey comprised three subsections, with each subsection asking questions that addressed aspects of cybersecurity within commercial banks. The respondents were presented with a five-point Likert scale option to select from. The first subsection required respondents to respond regarding their responsibility within the commercial banks concerning cybersecurity; the second subsection interrogated the respondents about their awareness of cybersecurity frameworks, policies, and procedures, and the last subsection aimed at incident response awareness within the banks. The respondents had to answer a total of sixteen questions.

4.11.2 Interview Structure

For the qualitative aspect of the study, a semi-structured interview was carried out with identified participants using video conferencing software (Microsoft Teams and Zoom). The semi-structured interview questions were not standard but rather questions developed to address the research questions and objectives of the study and to understand better cybersecurity views and perceptions within commercial banks in South Africa. The survey was designed to take between twenty to forty-five minutes at most. The interview guide consisted of three sections: an information sheet containing the informed consent, background information on the study being conducted, and the researcher conducting the study.

The second section of the guide was the demographic information section. This section, similar to the section in the survey instrument, was meant to gather demographic information about the participants, such as their educational background, ethnicity, current job title and overall experience within the IT domain. The last section of the guide comprised questions the participants were asked to answer concerning their experiences. This comprised nine main questions. The first question was about the participant's awareness of cybersecurity challenges faced by the institution. The second question was about the participant's perception of why banks continued to suffer from cybersecurity threats and attacks, and the third was about the effectiveness of cybersecurity frameworks in protecting the institution. The fourth question was about the role human behaviour played in the development of cybersecurity frameworks, the fifth was about the impact cyber-attacks and threats had on the operation of the bank, and the sixth question was about the participant's awareness of the interventions in place to protect and mitigate the threats faced by the bank. The seventh question was about the participant's perception of how human behaviour influenced the development of cybersecurity frameworks within the bank; the eighth inquired about the perceived impact cyber-attacks and threats have on the operation of the bank, and the last question was centred around how well they thought cybersecurity was being factored into processes within the bank.

4.12 The Pilot Study

Ruel, Wagner and Gillespie (2016) describe a pilot study as a tool whereby researchers can ensure that questions are articulated well, as well as discern whether the response options are relevant, comprehensive, and mutually exclusive, not just in their estimation, but from the point of view of the respondents as well. The pilot study was used to assess the validity of the survey. A pilot study assessed the quality of the interview and survey instruments. It was performed on a small subset of the sample population. Four participants were chosen for the interviews for the pilot study, and ten people were selected to participate in the survey. The intention was to ensure that the interview questions and survey instruments operated well and elicited the correct information from the participants and respondents (Bell & Bryman, 2011). Data collection in the pilot study phase was akin to the proposed collection method for the larger population to ensure that the data collection approach would suffice for larger populations.

4.12.1 The Interview Guide

Three participants from the sample population were selected for the qualitative aspect of the research study for the pilot testing of the semi-structured interview guide. From these three participants, the researchers gathered data about the effectiveness and validity of the interview questions. The interviews were conducted using video calling software (Zoom), and the participants' responses were recorded.

The participants stated that when it came to attacks and threats, it would be better if the questions were broken down into external and internal threats, in particular, question five of the interview guide. This question could be asked multiple times from different perspectives of threat and attack. The participants also felt that they did not have a clear understanding of what was meant by a cybersecurity framework, as there was feedback about a framework being explained at the start of the interview to serve as a point of reference for the rest of the interview. In the seventh question, the participants stated that human behaviour was too broad a category and that it would be better to distinguish between employees and customers.

The overall feedback the participants gave painted a picture of ambiguity concerning the wording and what was expected from them in the responses. The questions were then altered to clarify threats and attacks from internal and external perspectives and address the ambiguity and the feedback gathered from the participants. Furthermore, an overview of what was meant by a cybersecurity framework was given at the start of each interview. During the interviews, it was also clarified that human behaviour encompassed both employees and customers of commercial banks. More extended questions were also split into shorter, more straightforward questions to make them easier to understand.

4.12.2 The Survey Instrument

The survey instrument, a subset of the sample population for the study's quantitative element, was selected for pilot testing. Ten respondents were used to test the survey instrument. An initial set of participants was identified, and then, using this initial set, they forwarded the survey to those they believed would be ideal respondents. At the end of the study, the respondents were asked to give feedback regarding the questions' clarity and offer suggestions. The survey was designed and distributed using Google Forms. It recorded the responses and the feedback from the respondents by having a compulsory feedback section at the end of the survey.

The feedback from the respondents highlighted how critical cybersecurity was to commercial banks and how they needed to protect their digital assets and investors. The respondents raised the issue of how the survey was distributed. They said that the study was flagged as malicious by some of the tools deployed on their company-issued devices, and in some cases, the link to the survey was blocked, and therefore participants could not connect to the study. The fourth respondent indicated that the formatting and the questions asked in the survey were generic and could be answered by anyone employed in commercial banks. The second respondent suggested including a question about detection and response capabilities within the banks. Two respondents said that the survey made them interrogate their knowledge of cybersecurity in general and how their current employers were addressing the issue.

Additionally, respondents expressed how some of the rules and policies put in place by their employers made simple tasks much more complicated. Learning was a challenge if the content they were trying to acquire was not on the employer's approved list of websites or content providers. Considering the feedback given by the participants, the language in the survey was changed to be as simple and as direct as possible, and compound questions were split into more straightforward single questions.

Questions about the perceptions of the detection and response capabilities of the banks were added, and a question was asked as to how inclined the participants would be to circumvent the rules to get tasks completed quickly. To address the challenge of the link being detected as malicious by security tools, the link was distributed to potential respondents' personal email addresses and published on social media. Furthermore, the researcher's details were added to the link to assure potential respondents of the legitimacy of the survey and to add an accountable party for any follow-up questions.

4.13 Data Analysis

Data analysis refers to the processes associated with deriving meaning and understanding from the various data sets collected during a research project as a basis for further action and theory building (Coghlan & Brydon-Miller, 2014). Babbie (2010) defined qualitative analysis as the nonnumerical examination and interpretation of observation to discover underlying meanings and patterns of relationships, and quantitative analysis was described as the numerical representation and manipulation of observations to describe and explain the phenomena that those observations reflected. Data analysis in mixed methods research involves analysing the qualitative data separately, using qualitative methods and tools and quantitative data using quantitative methods and tools. It also combines both databases using approaches that mix or integrate the quantitative and qualitative data and the results (Creswell & Plano Clark, 2017).

Within mixed methods, data analysis can occur at a single point or multiple points throughout the mixed methods research process. It also involves specific steps undertaken by the researcher and critical decisions made at different steps (Creswell & Plano Clark, 2017).

4.13.1 Data Analysis Tools

Data analysis tools aid researchers in making sense of the data collected. It makes reporting results and interpretations possible (National Association of Geoscience Teachers, 2017). How data is analysed depends on the study's goals and the type of data collected. For qualitative data, the researcher might analyse the data collected as the research progresses, continually refining and reorganising in light of the emerging results. For quantitative data, the analysis can be left until the end of the data collection process, and if it is an extensive survey, statistical software can then be employed (Dawson, 2009). Regarding data analysis, computer programs can help with the process. They can assist the researcher in interpreting and validating the data and the results.

The steps for both qualitative and quantitative data analysis, as stated by Creswell and Plano Clark (2017), are:

- Preparing the data for analysis,

- Exploring the data,
- Analysing the data,
- Representing the analysis,
- Interpreting the analysis,
- Validating the data, and
- Interpretation of the results.

These steps occur linearly in quantitative research but are often implemented simultaneously and iteratively in qualitative research (Creswell & Plano Clark, 2017). Numerous tools can be used for data analysis in qualitative data analysis. The researcher first has to prepare the data by transcribing text from interviews and observations into word processing files for analysis, with the preferred approach being the researcher creating verbatim transcriptions of the data. Various qualitative data analysis software programs, such as MAXQDA and Atlas, can consume the data.ti[10], Nvivo[11], or QDA Miner[12].

For quantitative data analysis, the researcher started by converting the raw data into a proper form, which included scoring the data by assigning numeric values to each response, cleaning the data entry errors from the data sources, and creating necessary variables. Multivariate analysis was employed to analyse the simultaneous relationships among several variables. Olkin and Sampson (2001) defined multivariate analysis as a statistical study of experiments in which multiple measurements are made on each experimental unit and for which the relationship among multivariate measurements and their structure is essential to the experiment's understanding.

4.13.2 Data Analysis Tools Of Choice

For the qualitative aspect of the study, Atlas.ti, in conjunction with Microsoft Excel and Otter.ai, was chosen. This was because the university had a licensing agreement for Atlas.ti and Microsoft Excel, and the researcher obtained a student subscription for Otter.ai. For the quantitative aspect of the research, a combination of tools was used for computation, analysis, and presentation of the results. The tools used were Python for data wrangling and computation and SPSS for the study and presentation, with Microsoft Excel also used.

[10] https://atlasti.com/
[11] https://www.qsrinternational.com/nvivo-qualitative-data-analysis-software/home
[12] https://provalisresearch.com/products/qualitative-data-analysis-software/

4.14 Mitigating Bias

Bias is becoming increasingly recognised as a genuine problem in many areas of scientific research. It is particularly of concern in cases where results seem to reflect the preferences and interests of certain actors involved in the research process directly (Wilholt, 2009). The researcher’s bias in this study was that at the time of the study, the participants were employees of a commercial bank in South Africa within the cybersecurity domain of the bank. To minimise bias, the researcher tried to ensure that in the early stages of the study, the researchers approached employees from other commercial banks outside of the one they were employed at to clarify that the study was not funded nor supported by any commercial bank. This minimised the perception that the researcher's employer was involved in the study. Furthermore, the researcher ensured that:

- They issued an information sheet to every participant or respondent of the interviews and the survey.
- They informed the participants that they did not need to provide any personal details that could identify them in the study, thus making their contribution anonymous.
- Their participation was entirely voluntary, and they could withdraw anytime.
- All the collected data was adequately masked and anonymised during the collection and analysis stage of the study.

4.15 Ethical Considerations

An application was submitted to the Humanities and Social Sciences Research Committee at the University of the Western Cape to adhere to strict ethical standards. The committee granted the researcher ethical clearance to conduct the study. The ethical certificate obtained from the university is attached as Appendix A. The identified participants and respondents of the study were requested to complete a consent form before participating. The consent form gave the background for the research and the reason the study was being carried out, and it also provided the ethical clearance reference number for the study. The main ethical concerns of the survey were privacy and confidentiality and adhering to the POPIA concerning the participants and respondents. The participants were fully informed about the study to address the ethical concerns. They were made aware of the purpose of the study, who or what group funded it, and how the findings from the study were to be used once it was concluded. They were also reassured that any personally identifiable information relating to them would be anonymised.

Participants were free to withdraw at any time without any negative ramifications. Furthermore, the data collected from study participants and any resources gathered were only available to the relevant parties. Great care was taken to mask the data to preserve confidentiality and anonymity when the information was distributed.

4.16 Chapter Summary

This chapter outlined the research design and methodology utilised in the study. It achieved this by briefly describing the various research paradigms considered for the study and focusing on the chosen paradigm, pragmatism. Secondly, it discussed various research designs within IS and highlighted the chosen research design, which served as the conduit to carry out the study. The target population, the sampling strategy, and the sampling size were also discussed in the chapter. A plan for analysing the collected data for the study and the tooling for the analysis were also discussed. Lastly, the chapter addressed how the study would mitigate the researcher's bias and described the ethical considerations the study would have to look out for, given the sensitive nature of cybersecurity within commercial banks. The next chapter presents, discusses, and interprets the qualitative data collected during the study.

PART IV

Chapter Five : Presentation And Discussion Of Qualitative Findings

5.1 Introduction

This chapter presents and discusses the study's qualitative findings according to the research procedures outlined in chapter four. The structure of the chapter is as follows: the first section discusses the participants' demographic information, the second section focuses on thematic data analysis, with the discussion of findings taking place within the presentation of the findings, and lastly, the researcher concludes the chapter. Qualitative data for the study was collected from Information Technology (IT), Risk, Compliance, and Legal professionals within the banking space in South Africa for seven months, from June 2021 until January 2022.

The participants were either full-time employees, contractors, or consultants within the banking industry in South Africa. The participants came from the well-established big five banks and smaller commercial banks within the country. Semi-structured interviews allowed participants to be probed beyond the prepared interview questions. These interviews were conducted on Zoom, and the interviews were recorded with the consent of the participants. Most of the interviews were voice-only calls instead of video calls because of bandwidth constraints and the preferences of some participants. This approach also ensured that the participant's identities were protected.

5.2 Demographic Profiles Of Participants

The data collected for the study was gathered from twenty-one participants, fourteen male participants and seven female participants. The disparity between the number of male and female participants was partly because males dominate the ICT sector within South Africa. This was supported by Padayachee and Pillay (2018), who stated that females are under-represented within the IT sector in South Africa, which was further evidenced by Malinga (2021), who pointed out that out of the 236 000 ICT roles within South Africa, females only hold 23 per cent of those roles. Consequently, the study has more male than female participants. Lee and Schuele (2010) stated that demographic information in research studies provides data regarding the research participants and is vital for determining whether the individuals in the study are representative of the target population and may be applicable for generalising to the population. Lazar, Feng, and Hochheiser (2017) supported this statement by positing that demographic data may be used to determine that responses collected in a study represent a diverse cross-section of respondents. Table 5.1 and Table 5.2 summarised the demographic details of the twenty-one participants who participated in the study. The participants' identities were anonymised to protect their information, and the researcher adhered to what the participants consented to as the study's ethical constraints. The participants were given simple, unique identifiers of the first letter of their first name and the first letter of their last names. Numeric characters were also added to the pseudonyms, starting at one and increasing to twenty-one, with increments of one. The table below summarises the participant’s characteristics, such as their gender, age group, highest qualification, years of experience within their field of practice, and their current titles at the time of the data collection.

Table 5.1 Demographics of participant

Participant	Male	Female	18-25 years	26-35 years	36-45 years	46-55 years	56+ years
DM01	1				1		
TM02	1				1		
NT03		1		1			
OO04	1				1		
KM05	1			1			
BN06	1			1			
HN07		1		1			
JD08	1			1			
AM09	1				1		
AB10	1			1			
MR11	1			1			
KS12	1			1			
RG13		1	1				
MN14	1			1			
JB15	1				1		
JP16	1			1			
SD17		1		1			
VS18		1		1			
AA19	1				1		
KR20		1	1				
NM21		1		1			
Total	14	7	2	13	6		

Table 5.2 Demographics of participants continued.

Participant	Highest Qualification	Job Title	1-5 years	6-10 years	11-20 years	20+ years
DM01	Higher Certificate in Management Practices	IT Operations Manager			1	
TM02	Certified Information Systems Security Profession (CISSP), Certified Ethical Hacker (CEH), Computer Hacking Forensic Investigator (CHFI), Certified Security Operations Centre Analyst (CSA)	Cybersecurity Specialist			1	
NT03	Bachelor's Degree	Internal Auditor	1			
OO04	Master's Degree	Cybersecurity Specialist		1		
KM05	Honour's Degree	Cybersecurity Specialist		1		
BN06	Master's Degree	Cybersecurity Specialist	1			
HN07	Master's Degree	Threat & Vulnerability Management Analyst	1			
JD08	Bachelor's Degree	Security Consultant	1			
AM09	Master's Degree	Senior Manager: IT Audits			1	
AB10	Bachelor's Degree	Software Developer	1			
MR11	Bachelor's Degree	Risk Specialist		1		
KS12	Bachelor's Degree	Information Systems Engineer		1		
RG13	Bachelor's Degree	Business Intelligence Analyst	1			
MN14	Master's Degree	IT Risk Specialist		1		

JB15	Bachelor's Degree	Chief Information Security Officer				1
JP16	Bachelor's Degree	Security Consultant	1			
SD17	Bachelor's Degree	Software Developer	1			
VS18	Honour's Degree	Head of Data Enablement		1		
AA19	Honour's Degree	Information Security Officer			1	
KR20	Bachelor's Degree	Data Security Analyst	1			
NM21	Bachelor's Degree	Business Service Lead			1	
Total			**9**	**6**	**5**	**1**

5.2.1 Gender

Seven females and fourteen males made up a total of twenty-one participants in the study. The intention was to have diversity in terms of gender because having variety offers different perspectives on matters. Bert (2018) stated that gender diversity in scientific research provides unique perspectives to study and scientific conversation. Nielsen, Alegria, Börjeson, Etzkowitz, Falk-Krzesinski, Joshi, Leahey, Smith-Doerr, Woolley, and Schiebinger (2017) further posited that considering gender within the scientific process may assist researchers in adding new dimensions to research. Real variations exist in the structural organisation of the brains of men and women, which may influence their responses to stimuli and events (Chigada, 2021).

5.2.2 Highest Qualification

Most participants (eleven) held bachelor's degrees, followed closely by those with master's degrees (five), and four participants had honours degrees. The results depicted that the cohort of participants identified for the study mainly possessed good formal education and, in most cases, held a formal qualification for their field or other professional qualifications recognised in their domain. Since these qualifications were centred around IT, the participants understood cybersecurity and its importance in information systems and technology. Collecting demographic information on respondents' educational backgrounds aids in assessing the level of skills and knowledge possessed by the respondents (Albert, Tullis, & Tedesco, 2009). This is particularly pertinent to cybersecurity, as the field spans various academic domains (Ramluckan, van Niekerk, & Leenen, 2020).

5.2.3 Age Group

The diversity in age offered different perspectives on the matter at hand. Thirteen participants were aged between 26 and 45 years, two were between 18 and 25, six were between 36 and 46, and none were aged 47 and above. This was because different generations might perceive cybersecurity and its challenges differently. Collecting data from varying age groups is valuable to research, as it brings together views from different generations, adding a wealth of complementary abilities, skills, information, networks, and varied opinions on matters. This is because age cohorts experience significant events and phenomena at similar points in time, and as such, having multiple generations represented in a study merges views and opinions that might otherwise not be captured by one specific generation (Gerhardt, Nachemson-Ekwall, & Fogel, 2022).

5.2.4 Years Of Experience

Nine of the participants had working professional experience that fell within the category of 1 to 5 years, and six had experience ranging between 6 to 10 years, followed by five participants who had experience between 11 and 20 years and finally, one participant had experience gathered over more than 20 years. The distribution of working experience showed diversity among the participants, which offered great insights from a range of expertise. Years of experience within the working world is a vital element that assists researchers in understanding whether the respondents possessed the necessary knowledge, experience, and exposure to address the research question adequately. This study's research questions sought those with experience in IT, cybersecurity, risk, legal, governance, or compliance (Salkind, 2012; Chigada, 2021).

5.2.5 Participants Job Titles

There were seventeen job titles among all the participants, with the most prominent job titles being cybersecurity and information security specialists. The job titles gave the researcher various views on cybersecurity within commercial banks, ranging from those with intimate knowledge of the subject to those unfamiliar with it, although they found themselves within IT. This further demonstrated that the study sought inputs from knowledgeable individuals who encounter cybersecurity policies, controls, and risks in their operational tasks.

5.3 Thematic Data Analysis

Petersen (2019) described data analysis as a method for a researcher to understand underlying reasons, perceptions, motivations, and consequences that emerge because of interrelationships between conditions and actions. Qualitative data analysis brings meaning to a wide range of qualitative data (e.g., conversational data, images, observations, and unstructured, semi-structured or structured interviews). It means various things to researchers as it is often aligned with a particular methodology, theoretical perspective, research tradition, school of thought or field (Lester, Cho, & Lochmiller, 2020). Qualitative data analysis is simultaneously an iterative and sequential process that follows several steps to assign meaning to pieces of data (Rossman & Rallis, 2017). This study employed thematic analysis to identify key impediments to the challenges commercial banks face in South Africa regarding developing local cybersecurity frameworks. Thematic analysis is a method used to identify and interpret meaning patterns across qualitative data (Clarke & Braun, 2014). The steps that were followed when analysing the data were based on Rossman and Rallis (2017) in conjunction with Creswell's Data Analysis Spiral (Creswell & Poth, 2017), which requires the researcher to taking an iterative approach to each of the steps while gradually moving forward with each step and leaving behind previous steps. The process was as follows:

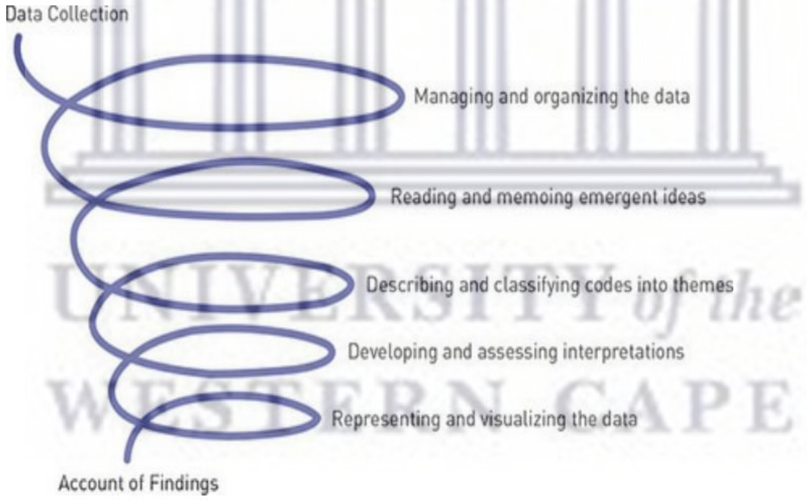

Data Collection
Managing and organizing the data
Reading and memoing emergent ideas
Describing and classifying codes into themes
Developing and assessing interpretations
Representing and visualizing the data
Account of Findings

Figure 5.1 Data analysis spiral

- Data organisation.
- Perusing the entire data multiple times to familiarise oneself with its contents. This process included making notes on possible categories or interpretations.

- Identifying general categories (codes) that Adu Field (2019) described as labels generated to represent the questions you want to address in your study. Create themes and subthemes and then assign the codes to those themes appropriately.
- Integrating and summarising the data.

Table 5.3 Themes identified.

Interview Question	Main Theme	Subtheme 1	Subtheme 2	Subtheme 3	Subtheme 4
What cybersecurity challenges are you aware of that banks face from an internal and external perspective?	Lack of skills	Lack of resources	Users with limited technical proficiency	Poor security culture	Misalignment of security and business
Which cybersecurity frameworks are you aware of within your bank?	NIST Frameworks	ISO Frameworks	Do not know	Custom frameworks	None
Do you know what benefits these frameworks offer and what they entail?	Provide guidance	Drives compliance	Improve investor confidence	None	None
Do you think the adoption of the current cybersecurity frameworks is effective in protecting the institution? What factors impede your bank from developing a practical cybersecurity framework?	The framework is effective	The framework can be improved	Not sure	None	None

Why do you think banks continue to suffer from internal and external cybersecurity attacks and threats?	Attractive target	Insider threat	Poor cyber hygiene	Poor cybersecurity culture	None
Which interventions do you know are in place to protect and mitigate the threats faced by the banks?	Security controls	Security tools and assessments	Awareness and training	Risk assessment	None
How do you think human behaviour contributes to developing cybersecurity frameworks in banks?	Human behaviour is a key input	Humans are key to the framework	None	None	None
How do cyber-attacks and threats impact the operations of the bank?	Stop operations	Reputational damage	Financial losses	Loss of investor and customer confidence	None
Do you think cyber-attacks and threats are considered at every stage of the bank's processes?	Security is not considered because security is a siloed operation	No, because business requirements come first	No, lack of awareness	Yes, security is considered in the design phase	None

5.3.1 Cybersecurity Challenges Faced by Banks from Internal and External Perspectives.

This question explored the challenges commercial banks face regarding cybersecurity, revealing one central theme raised by most participants and four other subthemes. The themes identified were:

Theme 1: Lack of skills

When participants were asked about their perception of some of the challenges faced by commercial banks regarding cybersecurity, the responses were as follows:

> *"I don't think that we have an all-round. I don't think I don't think the industry has an all-around pool of skilled people that can effectively, you know, defend, to a certain extent, yeah."* (Participant MN14)
>
> *"I think one of the challenges as well is kind of skills, because when it comes to, so I also studied IT, but when I showed interest in IT security, but when it comes to the actual work, you know, the actual analytical kind of work that I'm currently doing, it's something that I wasn't taught, you know, in varsity, and it's something, it's a new skill that you acquire when you're in cyber."* (Participant HN07)
>
> *"They will always face threats internally and externally for exploitation and resourcing. I think resourcing. Yeah, because we are not sure, like in South Africa, we say that we are a country with such high unemployment, but there's always this case where we are under-resourced. It's a question of the right skills or the right level of skills to be able to protect the bank."* (Participant MR11)

The extracts demonstrate that some participants were aware of the lack of cybersecurity skills. They explained how lacking such a fundamental skill was detrimental to an organisation's security posture. Kshetri (2019) mentioned the lack of cybersecurity skills and estimated that by 2020, there would be a shortfall of about 100000 cybersecurity personnel in Africa. The World Economic Forum (2022) and (ISC)^2 (2021) stated that there is still a workforce gap of more than 2.72 million positions globally and that the cybersecurity workforce needed to grow by 65 per cent to defend the critical assets of organisations effectively.

Theme 2: Lack of resources

Participants also noted a lack of resources as one of the driving forces behind the challenges faced by commercial banks. The lack of resources ranged from insufficient investment in research and development to insufficient financial support from executives and inadequate tooling. The responses of the participants are below:

> *"I think the budget would be one of the biggest challenges. And I'm saying this is remembered mostly because the organisation is the bank itself. By its nature, it's huge, right? So, for them to properly ensure that the bank is protected, and such, so the question is, do they have enough budget?"* (Participant TM02)
>
> *"And under-resourcing leads to a plethora of issues in terms of they can't deal with the vulnerabilities in a timely manner. They can't keep up with technologies; they can't keep up with security training."* (Participant MR11)

> *"And the other challenge or the underlying challenge was lack of resources. So, you have fewer analysts or engineers, looking at a SOC."* (Participant BN06)

The participants highlighted a lack of resources as one of the subthemes that contribute to the challenges faced by commercial banks regarding cybersecurity. The lack of resources included insufficient funding regarding the size of the budget apportioned to security, and the other resources included inadequate staffing of cybersecurity personnel. The European Union Agency for Cybersecurity (2021) supported the participant's views by positing that a lack of information security awareness and expertise in organisations often leads to a lack of cybersecurity budget and inadequate staffing.

Da Veiga *et al.* (2020) stated that resources are required for successful implementations or changes to information security within organisations; budgeting and funding are crucial to implementing security practices. Their study also highlighted a lack of resources as one of the most significant obstacles for organisations to improve information security.

Theme 3: Users with limited technical proficiency

Commercial banks' cybersecurity challenges are industry-wide and not specific to one commercial bank. One of the subthemes a considerable number of participants mentioned was about users with limited technical proficiency who were part of the challenges commercial banks face from an internal and external perspective. The responses are captured below:

> *"The second part of it, which is a lot around education and awareness and training for your staff, is that your staff need to be aware of the type of emails; they need to look out for the type of phishing emails being sent. It's very well crafted these days."* (Participant AA19)

> *"Yes, we put controls in place to ensure they cannot remove that sensitive data information. But they are our first line of defence. And our first point to the kind of challenges out there with regards to, you know, being bribed to plug in malicious devices, or to be able to exfiltrate out data for specific whatever they call it, I think of the word now that the attackers use a syndicate, Syndicate, and that's always going to be the main thing."* (Participant JP16)

> *"The biggest vulnerability, according to me, right? It's people. Yeah, it's people. And, and by people, I mean end-users, because those are where most of the breaches stemmed from, you know, you're phishing and all that."* (Participant KS12)

Some major cyber incidents that have occurred recently were partly due to incompetence, negligence, or users who did not know better. This was evidenced by van Niekerk (2017), who stated that one of the first successful cybercrime incidents against a commercial bank was a threat actor compromising a user's account by sending malicious mail to a user. This was not the last occurrence where threat actors viewed end-users as viable threat vectors. Over the years, countless other attacks have used unaware and negligent users to enter organisations. Mitnick *et al.* (2002) stated that employees and end-users are the greatest threat to corporate information security, whether intentionally or through negligence or often due to lack of knowledge.

Theme 4: Poor security culture

Participants identified the deprioritisation of cybersecurity as one of the contributors to the challenges commercial banks face regarding cybersecurity. This led to occasions where organisation security was treated as a tick box exercise. No traction on security matters was achieved because of inadequate senior buy-in to driving security objectives.

> *"The first issue is that the executive is primarily focused on generating revenue, as opposed to implementing security controls"* (Participant JB15)

> *"I think it's because I'm in, I've been put in a position where it's not emphasised, cybersecurity, let me put it this way, like, within a system, it feels like we are all given different titles. And when you're given a title, you stick to the title and like expectations, and our theory to sort of know or understand it and things."* (Participant SD17)

> *"I mean, a long time ago, not maybe a long time ago, not a long time ago. But if I were to wrap it up, I'd say it before, it wasn't something that banks traditionally focused on*." (Participant NM21)

Security prioritisations help organisations identify the potential risks affecting them and prioritise the defence of their digital assets (Blum, 2020). In their responses, the participants mentioned that security had only become a consideration recently. Although the participants might occupy high positions of influence, security was still not emphasised in their role, implying that their subordinates also did not see the importance of safety. Keman and Pearlson (2019) stated that an organisation's lack of a strong cybersecurity culture can make them less resilient against cyber-attacks. Also, an organisation's robust cybersecurity culture significantly improves employees' inclination to adhere to cybersecurity controls.

Theme 5: Misalignment of security and business

The following subtheme identified a trend where participants felt that cybersecurity and business were not aligned and that the two objectives were not similar. The responses from the participants that highlight that are as follows:

> *"If you have too many security controls in place, you're slowing down business and stopping business from happening."* (Participant JB15)

> *"But remember, security is a deterrent to business. To a certain extent. That's why you can't. We can just put encryption on everything because it degrades the performance of applications. So, we always need to see how best we can apply encryption, for instance, to such an extent that it doesn't necessarily degrade application performance. However, it's still there in the right interaction points, that data won't be compromised, and service won't be compromised."* (Participant KS12)

> *"You know, and this is the big kind of the elephant in the room with security is that security is always seen to business and project drivers as a blocker."* (Participant JP16)

The misalignment of business needs and cybersecurity often leads to a misunderstanding of cybersecurity's role in organisations and its impact on helping organisations deliver their products and offerings. Blum (2020) stated that misalignment of security and business could negatively affect any project's protection. Edwards (2020) said there was a disconnect between how businesses understand and manage cyber risk and how staff understand it. That is driven by organisations failing to view cybersecurity as a business strategy rather than an IT problem. Due to this limited scope of cybersecurity, an organisation's ability to analyse cyber risks and prioritise and execute remediation based on business criticality and the threat context is hampered. To overcome this misalignment, Boehm, Curcio, Merrath, Shenton, and Stähle (2019) posited that organisations needed to move towards a risk-based approach to cybersecurity, which would enable organisations to identify, prioritise, deliver, manage, and measure security and privacy controls, based on an agreed-upon enterprise risk management framework; simultaneously including stakeholders from the organisation regarding cybersecurity operations.

5.3.2 Cybersecurity Frameworks Within Your Bank

The above question sought to determine employees' familiarity with the cybersecurity frameworks used within their organisations. From the question asked, one central theme emerged concerning how familiar the employees were with the framework of their organisation. Three other subthemes emerged from the interviews:

Theme 1: NIST Cybersecurity Framework

Multiple participants mentioned the NIST and the CSF as the frameworks used within their organisations. Although sometimes not explicitly stated by the organisations, the participants recognised the framework through some of the characteristics and controls it imposed. The responses of the participants are captured below.

> *"So, the NIST, I know we are just at the company that I'm working, for now, we just did NIST, NIST review."* (Participant MR11)
>
> *"Okay. All right. So, what I know is okay, this is the NIST framework."* (Participant AM09)
>
> *"So, for most of everything, I've based everything on NIST compliance. Okay. The reason I've chosen NIST is that the American government takes federal law very, very seriously"* (Participant JB15)

The NIST's cybersecurity framework is a set of everyday cybersecurity activities across the critical infrastructure sector. The framework presents industry standards, guidelines, and practices that allow communication of cybersecurity activities and outcomes across organisations, from the executive to the implementation/operations level (Alexander & Panguluri, 2017). This framework is one of the most widely used frameworks within cybersecurity. It offers standards and implementation guides by recommending controls and practices organisations can implement to secure digital assets. Estimates state that almost 50 per cent of all enterprises used NIST, the framework being the most mentioned by participants, showing its popularity and widespread adoption (Banga, 2020).

Theme 2: ISO Frameworks: Participants also cited the International Organization for Standardization (ISO) standards as a framework they were aware of within their organisations. Although some participants could distinguish between standards and frameworks, most of the participants saw no difference between standards and frameworks. The responses of the participants are quoted below:

> *"Like sort of standard, like, for example, the one that I'm aware of. It's ISO 2700 something"* (Participant NT03)
>
> *"The ISO 27001 is the only internationally accepted framework. So, meaning that it's an ISO standard, it's accepted everywhere is used everywhere, and that is the accepted norm."* (Participant KM05)
>
> *"Then your ISO to 27001 And 27002, and then. Yeah, but then now also, with the cloud. This standard is an ISO standard for security in the cloud."* (Participant AM09)

The ISO 27001/ISO 27002 frameworks/standards describe an ISMS and detail the steps involved in the establishment of such a system, whereby the ISMS aims to minimise risk and ensure business continuity by limiting the impact of security breaches through creating policies and procedures to manage a business's sensitive information. The ISO 27000 cohort of standards intend to enable various organisations to manage the security of assets such as financial information, intellectual property, employee details or third-party information (International Organization for Standardization, n.d.).

Theme 3: Do not know (Unaware): A subtheme from the interview with the participants was that few were unaware of the frameworks utilised within their organisations. Participants gave reasons ranging from cybersecurity not being in the direct scope of the roles they were employed to occupy in the organisations they worked for to their employers not emphasising cybersecurity enough in their day-to-day operations. The responses of the participants were as follows:

> *"I'm not really familiar with. I think it's because I'm in, I've been put in a position where it's, it's not emphasised."* (Participant SD17)

> *"I actually don't know. It's not in my scope. And then I've not really seen or heard anything shared along if the exact frameworks or tools that are being used within the bank."* (Participant DM01)

> *"Zero, sorry. I guess more I don't know if I should call front-end or client-facing software; those layers might integrate more directly into our cybersecurity framework. But we are the absolute back end."* (Participant AB10)

Theme 4: Custom frameworks: The final subtheme from the participants' comments was how some commercial banks created custom frameworks that relied upon existing frameworks adapted to meet their specific requirements. Although this occurred as a subtheme, only a handful of participants mentioned it. The responses are shown below:

> *"So, there's the Reserve Bank. Obviously, we've got to take into account regulations, like GDPR regulations, like POPIA and GDPR. And then, like, those are the primary ones that we use. But there's obviously pulled other data from other frameworks for my policies, so I've also pulled in a little bit of CIS, have pulled in a little bit of SANS, and a little bit of, like, OWASP. In terms of standards, and then the other standards are all just said, driven by the regulator."* (Participant JB15)

> *"From a framework perspective, we are mostly aligning to ISO your NIST, but it's a blended framework type view. But what the bank has decided to do is to move away from trying to be compliant with certain standards. And what we do is we've taken an intelligence-led approach, where we use a risk and viability framework."* (Participant KS12)

> *"So, we use a combination. I'm not going to say that we replace everything with one, but we use a combination of CIS benchmarks, NIST, and ISO. There are obviously frameworks and things that get kind of pushed to us from a reserve bank perspective regarding, like, Cloud directors, those types of things, which we still have to meet with, so that's really a combination of things."* (Participant JP16)

5.3.3 Benefits Offered by Frameworks.

The above question was posed to participants to elicit their knowledge of the frameworks employed within their organisations. The intention was to uncover whether the participants knew intimately about the framework they worked under and what it entailed. However, the question depended on the participant's awareness of the framework. In some instances, the question was not applicable as participants had indicated in the previous question that they did not know what framework was employed in their respective organisations or, sometimes, even what a cybersecurity framework was.

Theme 1: Provide guidance: The central theme that emerged from the question was that participants viewed the role of the framework within the organisation as one that guided cybersecurity practices and controls. The guidance given by the framework could also inform the behaviour of employees within the organisation. The responses of the participants are shown below:

> *"It gives you a conceptual idea of what the landscape looks like. And what are the pillars that you need to be focusing on? And a guide as well, you get serves as a guide to, you know, instruct you and point you to the right direction."* (Participant MN14)

> *"My understanding of frameworks is that they provide guidelines to optimise a particular area. I'm not a specialist when it comes to frameworks. So, I do know that there are benefits once they've been through your frameworks, you get to your processes, you get your procedures, and you get your standards and stuff like that."* (Participant OO04)

> *"Previously, your NIST tends to lean towards a more technical approach to cybersecurity, especially around encryption, the way you go about protecting your perimeter, protecting yourself internally from a workstation perspective, from a server perspective, what are the hardening standards around that, so NIST tends to lean more towards the technical how to go about putting these controls in place. And if I look at the ISO standards, the ISO standards map out the controls that you need in place to ensure that you can state that you actually comply to some sort of security management system."* (Participant AA19)

The views held by the participants aligned with the existing literature around cybersecurity frameworks. The frameworks and standards are recommendations for securing organisations or critical infrastructure. In most instances, the frameworks are technology agnostic and leave the decision of choosing vendors and tools up to the implementor. Copan (2020) supported this, stating that the NIST cybersecurity framework is designed to be vendor-agnostic.

Still, it intends to help organisations create the building blocks needed to secure the organisation. The Open Group (2017), responsible for the O-ISM3 framework, also stated that the framework was intended for managing information security and ensuring that security processes operated at a level consistent with business requirements. It adopted a technology-neutral stance and focused on standard information security processes.

Theme 2: Drives compliance: Participants stated how some cybersecurity frameworks ensured their organisations complied with specific international or local standards and requirements. The participants mentioned how compliance with some standards improved the organisation's reputation and helped it align with its peers.

> "*ISO standards, the ISO standards map out the controls that you need in place to ensure that you can state that you actually comply to some sort of security management system."* (Participant AA19)

> *"So, another advantage is so an organisation will be complying with regulatory requirements. So, if they don't, obviously, there's a fine. If they don't, there's also reputational risk."* (Participant AM09)

> *"That is the only internationally accepted framework. So, meaning that it's an ISO standard, it's accepted everywhere, is used everywhere, and that is the accepted norm."* (Participant KM05)

The ISO/IEC states that certification with their standard may be a valuable tool in adding to an organisation's credibility as it demonstrates that the organisation meets specific customer requirements and expectations and, in some instances, legislative requirements. Compliance with standards such as the Payment Card Industry Data Security Standard (PCI-DSS), which is a requirement for all entities that store, process, or transmit cardholder data, demonstrates to customers and regulatory bodies that the organisation has taken steps to secure sensitive data relating to payments and has taken measures to adopt consistent data security measures that are in line with global standards (Payment Card Industry Data Security Standard, 2022).

Theme 3: Improve investor confidence: Closely related to the benefit of compliance with the frameworks was the impact the frameworks had on investor confidence. The adoption of frameworks positively contributed to investor and customer confidence. The participants highlighted how the indirect effect of the frameworks sometimes led to better customer retention. Furthermore, the frameworks assisted in protecting the data and intellectual property of the organisation, which had a good influence on investor confidence.

> *"Even things like customer retention, because banking for anyone to bank with a bank, they've got to trust that the bank, they're gonna trust that the bank is secure."* (Participant AM09)

> *"So, it is more about delivering value to the business while also then being cognizant of the fact that we need to, you know, protect our data. But data is actually the last thing, although it's not like we are ignoring it."* (Participant KS12)

> *"The benefit of that, obviously, to protect our clients and also as the whole company as a whole, to protect us from outsiders or competitors that may use the information to steal our business or may use the information to corrupt or damage our data."* (Participant RG13)

The themes that emerged from the question were supported by Kosutic and Federico (2020), who stated that cybersecurity contributed to creating business value by driving compliance with regulations and industry standards and reducing the number of cybersecurity-related incidents. These improvements increased market value by positively influencing stakeholder perception and improving customer satisfaction.

5.3.4 Adoption of Cybersecurity Frameworks and Factors Impeding the Bank from Developing an Effective Cybersecurity Framework?

The above question sought to determine the participant's views on the effectiveness of the adopted framework. Simultaneously, it sought to find out what impeded the organisations from developing their frameworks if the ones they adopted were not proving to be effective.

Although most participants could not confidently answer the question due to their limited knowledge of the adopted framework, three themes emerged from those who could answer.

Theme 1: The framework is practical: Most participants believed the adopted framework had effectively protected the organisation. Some participants based this view on the fact that their organisation had not recently suffered significant material incidents. Conversely, others believed the framework had been practical because it gave the organisation a sense of direction in securing digital assets and their processes. The responses of the participants were:

> *"The adoption of the framework has been instrumental Yes. To assisting the institution to know exactly which direction to take."* (Participant KM05)
>
> *"Um, yes, I do. I think, you know, like I said, as a big bank, we are more regulated to doing things than just beside what we want to do."* (Participant JP16)
>
> *"Think they have, I think they have, given that we haven't had data leakage."* (Participant NT03)

Theme 2: The framework can be improved: Some participants stated that, although the current framework had effectively protected the organisation from catastrophic cyber-attacks, there was still room for improvement. They said cybersecurity was a moving target, and the organisational culture around cybersecurity needed to change for the frameworks to improve. Others mentioned some of the controls the framework had presented and how they had helped secure the organisation and protect its clients. Here are the responses:

> *"So, my question in a convoluted way is, to a certain extent, but not 100% coverage, like they don't have 100% protection to the organisation. I just feel like it's more like a tick box exercise, either to comply with regulatory policies or whichever policies might apply to the bank."* (Participant TM02)
>
> *"Yes, to a certain extent, it has been effective. I'll give you an example. The cybersecurity framework spoke to us expects the right word is recommended that you have multi-factor authentication within an environment that provides a level of protection in such a way that you, a user or a user, are expected to have two forms of authentication, which is what you know. Perhaps what you have enables a high-level of baseline security, which, if there is an attack, the user can the user's credentials may be stolen. Still, because the attacker does not have the second factor of authentication, they will not be able to effectively compromise their account."* (Participant OO04)
>
> *"To a certain point, yes, it has been; I mean, we still have frameworks in place, but how many people do follow that how many people really take the literal act of protecting customer information?"* (Participant RG13)

Theme 3: Not sure: Another subtheme from the question was the participant's inability to comment on the framework's effectiveness. This subtheme spoke to how cybersecurity was often siloed away from IT professionals who would perhaps benefit from knowing about the framework they operated under. Some participants said that since cybersecurity was not directly in their scope of work, they could not say whether the framework was practical. Their responses are shown below:

> *"I wouldn't be able to answer that confidently. Again, because it's not really in my scope."* (Participant DM01)

> *"I don't know. So, for me, I know you see now. I don't know. Okay. I don't know, honestly."* (Participant VS18)

5.3.5 Internal And External Cybersecurity Attacks And Threats

This interview question was intended to probe the participants about what they viewed as the reasons behind the attacks that commercial banks continued to face. The themes of the question varied from technical shortcomings to external factors beyond the institutions' control.

Theme 1: Attractive target: The central theme that emerged from participants was that commercial banks continue to suffer from attacks and threats because cybercriminals viewed them as attractive targets. Participants expressed that banks hold money which has immediate value to criminals but also significant amounts of personal data which, if exfiltrated from the organisations, could be sold on the dark web to other criminals for money, or the data could be used for other attacks where stolen credentials would be necessary or where the stolen personally identifiable information could be used for sophisticated phishing attacks. The responses of the participants were:

> *"I think the reason why they continue to suffer from attacks has to be the data that they hold financial data. So that is worth gold to them."* (Participant MR11)

> *"I mean, the bank deals with money, you know. So, because of that, it will always be constantly attacked from cyber."* (Participant TM02)

> *"I work in a financial institution, any attacker that can compromise, the institution can steal money can steal information about customers that they can sell."* (Participant OO04)

Cater (2017) supported the participants' views, who reported on the recent increasing number of cyber-attacks financial services faced. IBM (2017) also reported that most cyber-attacks in

2016 were aimed at the financial services sector. These views aligned with the participant's opinions that banks are attractive targets for cybercriminals.

Theme 2: Insider threat: Participants cited insider threats as one of the reasons banks continued to suffer from attacks. Some participants indicated that insiders are more challenging to monitor as, in some instances, the employees(insiders) already have keys to the kingdom, and their nefarious activities cannot be easily differentiated from legitimate activity. The other concern participants raised was that employees often lacked the necessary cyber awareness to act appropriately in the face of cyber threats.

> *"So, you know, really hard to find an insider, right as compared to something external, because the insider already has access to many of the tools being used. It's tricky to find an internal person like you never suspect a family member, you know, you'd always look outside only to find that, you know, the inside."* (Participant HN07)

> *"You get disgruntled employees, people who intentionally feel like I didn't get a raise, I didn't get the increase that I wanted. Therefore, I can actually do this; I'm justified; those are like very dangerous people; you have to actually look at that."* (Participant KM05)

> *"The internal one, I think it would be as a result of disgruntled employees; you don't want someone who's not happy; they obviously gonna do something. And then also, if the bank takes time to remove someone who has left the organisation in a workplace, we, we stand a chance at being at risk of that person using the information or just manipulating anything, because they're no longer part of the organisation, but still have access to the organisation."* (Participant NT03)

Cases of insiders(employees) being a threat to organisations are well documented in the literature. Keman and Pearlson (2019) stated that insider threats from human behaviour are among the most challenging aspects of security control. Recent cases include a 2021 incident where an Absa employee allegedly defrauded the institution of ZAR 103 million. The employee was employed as a specialist engineer Buthelezi (2022). The employee's ability to carry out the transgression reinforces the participants' views that it is hard to detect malicious behaviour internally.

Theme 3: Poor cyber hygiene: The second subtheme that emerged from the participants was how poor cyber hygiene contributed to why organisations suffered from cyber-attacks. The participants explained how, in some instances, legacy systems that were not being maintained were in place, as well as poor technical hygiene that contributed to the security posture of the organisations. The responses are:

> *"But the other thing that we shouldn't, from internal, we shouldn't ignore is the lack of technical hygiene, that is very important people get it because they just don't take care of the environment as they should. It's a simple thing patching that patch should say that Microsoft releases very important, those making sure that you don't just get updates because you feel tired."* (Participant KM05)

> *"South Africa is a little bit slow to adapt, particularly to something like micro-segmentation. So, what we're seeing is still flat networks."* (Participant JB15)

> *"As you know, across companies in South Africa, there's a lot of legacy systems that in place, right, systems that were written with code that doesn't exist anymore, or code that is, you know, that wasn't reviewed properly."* (Participant AA19)

Kaspersky Labs describe cyber hygiene as steps that users of computers and other devices can take to improve their online security and maintain system health. It is about forming good habits around cybersecurity to stay ahead of cyber threats and online security issues (Kaspersky Labs, 2022). ENISA (2016) likened cyber hygiene to personal hygiene. They stated that once those habits are sufficiently integrated into an organisation, they would become simple daily routines and good behaviours that ensure the optimum online health of organisations. Such, Ciholas, Rashid, Vilder, and Seabrook (2019) stated that getting the basics right by applying essentials like patch management, malware protection, and secure configuration proved a practical approach to mitigating the threats and vulnerabilities organisations face.

Theme 4: The lack of cybersecurity awareness: The final subtheme that emerged from the participants was how a lack of cybersecurity awareness could be one of the factors why commercial banks continue to suffer from cyber-attacks. That could be attributed to inadequate training and awareness of being secure. The participants expressed how the end-users of information systems were usually the weakest link in the cybersecurity chain. The responses that highlighted such sentiments appear below:

> *"Remember, when all is said and done, right, the weakest link in the chain will always be users, right? So, one of the reasons why the bank would kind of like suffer all these cyber-attacks is, is there adequate training with regard to users? That's number one, right? And then number two would be, do we have enough preventative controls implemented within the bank?"* (Participant TM02)

> *"There is no awareness. I don't know whether there is awareness, maybe the people that you know, do these kinds of fraudulent activities that, you know, in security, we've got this tool, this tool, this tool, so they're doing it from a lack of awareness because they think they won't be caught, you know, because as much as there is security with awareness, but it's really security awareness when it comes to phishing when it comes*

> *to all those other forms of threats that we can experience from external."* (Participant HN07)
>
> *"So, that's your insider threats? Yes. I think so of one of the things I look at it's the core issue of, yeah, also seeing that seen as a core issue, I think it boils down to employee, your people awareness, or employee awareness, simply security awareness. So, obviously, you can deploy or configure your security controls. But if people don't understand the fundamentals, the risk, the threats, and also the impact to the business, they don't understand those things, then your controls, your controls cannot work in isolation, assuming that we prevent nefarious activities or malicious or malicious behaviour from users."* (Participant BN06)

One such instance is the Carbanak attack, a remote backdoor designed for espionage, data exfiltration, and to promote remote access to compromised machines. Carbanak targeted several banks and financial institutions globally, resulting in organisations losing up to 1 billion USD. The attack was achieved through spear-phishing emails (Kaspersky Lab, 2015). The use of spear-phishing to infiltrate financial organisations is an example of employers not being adequately aware and trained in cybersecurity. Uchendu *et al.* (2021) highlighted security awareness and training programmes as one of the critical factors that influence cybersecurity within an organisation, and this was further supported by Veiga *et al. (2020)*, who also expressed that security education training and awareness are crucial factors in building a robust cybersecurity culture within an organisation.

5.3.6 Interventions To Protect and Mitigate The Threats Faced By The Banks

Various interventions that informed the themes of the question emerged during the study. These included implementing controls within the banks, building a more robust culture and awareness around cybersecurity, and continuously monitoring and maintaining organisations' security posture. The themes identified during the analysis of the captured responses are shown below.

Theme 1: Security controls: Many of the participants indicated that having controls in place is one of the most effective ways to mitigate the threats and attacks faced by the bank. These controls comprise the three common cyber control types: physical controls, technical controls, and administrative controls (Chapple, Tittel, & Stewart, 2021). The responses were:

> *"So, we had initiatives around securing the perimeter and network. And then so obviously, making sure that we don't have any high-risk vulnerabilities that are externally facing, conducting pentest remediating vulnerabilities during the configuration, or on externally facing appliances are up to standard, and they don't*

> *have any vulnerabilities, the main reducing the attack surface, meaning that we don't have any vulnerable machines."* (Participant MR11)
>
> *"But, you know, as I said, we have controls in place to ensure that we monitor data flow and understand what's happening in the environment. And we also have a risk tolerance that we can work within. We are not silly enough to know that, you know, data breaches internally aren't going to happen. They are going to happen; we just must manage it accordingly and ensure that we have the correct monitoring and things in place."* (Participant JP16)
>
> *"Your data is your core; I mean, that is the critical component of your company; it is your crown jewel, so you protect your data. So, you make sure that from a layer perspective, as I explained coming in, if you look at it from the data moving outwards, you will look at, you know, the type of technical encryption measures that you have in place for data at rest. You look at the type of access governance that you also have in place, which means only certain individuals are allowed to have access to certain data at any given time"* (Participant AA19)

IBM Cloud Education (2019) describes security controls as 'parameters implemented to protect various forms of data and infrastructure important to an organisation. Any type of safeguard or countermeasure used to avoid, detect, counteract, or minimise security risks to physical property, information, computer systems, or other assets is considered a security control.' Although the participants stated that having controls in place is one of the best ways of mitigating the threats organisations face, inadequate controls or control failures are usually the reason behind successful breaches. Organisations must undertake a risk analysis to adequately put in controls to defend against attackers and determine the necessary controls to implement.

Furthermore, to guide implementation following best practices such as CIS Controls, which are a set of prioritised actions that form a defence-in-depth approach to security, could assist in reinforcing the controls in place and ensuring that when one control fails, there is another control or observability tool in place to substitute for failing controls.

Theme 2: Security tools and assessments: This theme was clustered around the various initiatives that institutions need to take to ensure that they are secure to some extent and that they continuously monitor their security posture to ensure that they have the proper controls in place and that they have appropriate risk mitigation strategies. This is necessary because participants view cybersecurity as a moving target in a world where technology is ever-changing. What was considered secure yesterday would not necessarily be regarded as secure today. The responses of the participants were:

> *"You know, interventions are definitely buying the latest and greatest technology, the bank, the banking institutions, or the sector, if you may, they, they hardly spare any expenses when it comes to tools"* (Participant MN14)

> *"We do a lot of simulation, penetration testing, continuous routine testing."* (Participant AA19)

> *"Two different vendors as perimeter security and the gateways like perimeter security and gateways. They use IPS, IPS and IDS technologies to do like virtual patching. They are using vulnerability scanners to pick up vulnerabilities that exist in the networks and in the infrastructure. They are utilising siems and soar technologies to proactively monitor events and soar technologies to build automated playbooks around those events. They're using third parties to help them understand their risks better."* (Participant JB15)

From the responses above, it was clear that the organisations use vast and varying tools from different vendors to protect them. Comments from participant MN show that organisations spare no expense when securing the best tools available. Tooling is integral to improving the visibility of what is happening within organisations and mitigating threat actors.

Security testing is also a tool organisations use to gauge their security posture and gather recommendations on securing their applications and digital assessments better. From the participants' responses, it is evident that organisations rely on penetration testing and third-party evaluations. Given the computer-based nature of cybersecurity, a combination of tools is needed to deal with the challenges in this space. These tools may be a collection of technical processes and practices designed to protect the institution (Möller, 2020). A list of some of the tools used is available in section 2.4.2.

Theme 3: Awareness and training: It was evident that security awareness and training programmes are crucial for educating end-users and employees. Hence, they become more aware of security threats and respond appropriately. Awareness programmes and training could range from employees watching videos, taking short tests on security, or taking part in phishing simulations where the organisation phishes them to judge their level of awareness regarding phishing or any other attacks that might be out in the wild. The responses of the participants are shown below:

> *"There so that it's really important awareness education with the customers as well, ensuring that they know that, you know, ever, if there's any communication that comes from a bank, that they verify that they trust in the source that it actually comes from."* (Participant AA19)

> *"We constantly have to do what is this cybersecurity trainings to just make sure that we are aware of, you know, is out there."* (Participant VS18)

> *"The people aspect, I would say the interventions have also been implemented there to ensure that you put people in those processes, that that that they understand their recommendations, that they understand they are role in protecting themselves and their organisations. You know, you can we can have awareness programmes, you can have awareness programmes, yes. That covers a lot of stuff, you know, depending on what the person does in the institution, you can have tailored content for those, you know, I would not, I mean, there's going to definitely going to be a general overlap, you know, from an awareness perspective."* (Participant KM05)

Security training and awareness programmes can be instrumental in maintaining an organisation's security posture and building a robust security culture. SANS (2021) stated that there has been a shift in security training, moving from a compliance-focused initiative to playing a crucial part in an organisation's ability to manage its human cyber risk.

Awareness programmes further assist in disseminating an organisation's security policy towards its employees in the hope that these programmes will encourage a security-aware culture so that good security practices will become the de facto approach to everything in organisations (Gundu, Flowerday, & Renaud, 2019).

Theme 4: Risk assessments: The final theme that emerged as a tool for protecting and mitigating the threats faced by the banks was risk assessments. Participants expressed how imperative it was for organisations to carry out risk assessment exercises. These assessments are critical drivers to understanding the overall risk organisations are exposed to and tools for calculating and understanding the risk they would be exposed to when integrating with third-party service providers.

> *"So, when I can think of taking that high-level risk assessment, being able to understand the risk faced by the bank, and through the process of risk assessment, you then need to make sure you have the right controls or tools, which mitigates those specific risk, and ultimately, threats as well."* (Participant BN06)

> *"For every third-party that we contract, we need to make sure that we do a risk assessment, including a cybersecurity risk assessment."* (Participant KM05)
> *Also risk management effective proactive for thinking looking risk management. I think banks have done a pretty good job in terms of trying to resource the risk management department."* (Participant MR11)

> *"Like I say, you're always going to have attacks and breaches, but this is exactly why we build in our risk appetite into these projects and how we implement controls, and we understand what is material to the bank."* (Participant JP16)

Blum (2020) posited that risk management can be a keystone within an organisation's security culture and governance model. He suggested using ISO 31000 risk management as a guide for business leaders to set the context for risk, carry out risk assessments and treatments and monitor changes in the organisation's risk profile. Wang, Ding, Sui, and Gu (2021) also supported the participants' views by stating that risk assessments are essential to effectively responding to cyber-attacks. Their paper demonstrated how risk assessments assisted in quantifying and identifying cybersecurity risks and finding attack paths, followed by high cybersecurity threats.

5.3.7 Human Behaviour's Contribution to The Development of Cybersecurity Frameworks in Banks

The question intended to gauge whether participants viewed human behaviour as essential to developing a cybersecurity framework. The participants were allowed to interpret this question however they felt appropriate. From the responses, two key themes were identified. The themes are presented below.

Theme 1: Human behaviour is a key input: From the participants' responses, it was evident that some participants considered it a key input in developing effective frameworks. Participants highlighted how any framework developed would need to consider how human behaviour could be counterintuitive to good security practices and posture. One even mentioned how the framework analysis depended on humans monitoring how other humans react and interact with specific controls in place. Humans in this question referred to the commercial banks' clients and the institution's employees because both parties played a role in upholding the institutions' security. The responses are shown below:

> *"I think, implementing these frameworks, its human beings, from an analysis point of view, seeing how other humans react or act towards everything in anything. So, I think human behaviour, seeing how people when someone has access to certain things and how they use the privileges, I think it contributes to the standard."* (Participant KR20)

> *"So, for external, I think human behaviour, it's really based for awareness, purpose purposes, right. So that they know that, you know, such and such happens, you know, especially in the financial institutions where you can be defrauded, you can, you know, find yourself in those tricky situations, and should this happen, you know, you need to*

> *contact the fraud team, etc., etc. But it's really, I think, to build awareness. That's where human behaviour kind of fits in."* (Participant HN07)

> *"You know, so in terms of the development of the, of the framework, so I believe that they would obviously take into consideration what I do put in my password they, and then they will take that into consideration, what are the risks that we bring when we do what we do putting our password out, via and then having a control framework that would actually cover all those risk exposures that we may introduce to the organisation."* (Participant NT03)

Theme 2: Humans are critical to the framework: The second theme highlighted humans' crucial role in cybersecurity. This theme centred on how humans interact with frameworks once developed and deployed in an organisation. Participants claimed a direct relationship between human behaviour and the framework, and others expressed how the psychological element around cybersecurity fed into the framework.

> *"I think these, it's actually quite important. If you read, you know, some of the thought leadership that comes out from your SANS or your ISACA from your ISC squared Institute's, they always say there's a massive psychological element to cybersecurity and especially how the human behaviour plays such an important part when you start implementing, you know, cybersecurity frameworks."* (Participant AA19)

> *"Yeah, I think there is definitely a relationship between the two. And I'm more inclined to say there's a direct relationship. Because we just tried to explain the sort of human behaviour. So, the frameworks will then need to cope with it to cater to human behaviour. It will be then a key consideration when developing this framework next. And so, I was going around in circles, just trying to tie things together. Yeah. But what I'm trying to say is that human behaviour needs to be considered because it's one of the key areas when developing these frameworks."* (Participant BN06)

> *"I mean, the human itself is important. Because nothing on that framework slash guideline is ever going to materialise without a human behaving a certain way or human being present a human behaviour to developing a framework"* (Participant MN14)

It is evident from both themes that human behaviour is a crucial attribute in cybersecurity frameworks. Human behaviour could loosely be attributed to an organisation's cybersecurity culture, and externally, it could be linked to cultural and societal views around cybersecurity.

5.3.8 Impact Of Cyber-Attacks and Threats on The Operations of Banks

The themes below served to answer the question above about the impact cyber-attacks and threats had on commercial banks. They also sought to meet the research objective of assessing the impact of cyber-attacks and threats on commercial banks. Four themes were identified from the interviews, as follows:

Theme 1: Stop operations: One of the other subthemes from the participants was the impact cyber-attacks had on the CIA triad mentioned in Chapter Two. Multiple participants commented on how attacks could impact either of the triad's pillars, leading to a halt in operations. The responses of the participants are below.

> *"I think from an attack perspective, if an attack is successful, the bank cannot operate at all. So, transactions cannot take place. People cannot transact, which leads to a financial impact on the bank."* (Participant MR11)

> *"They, I mean, it can really shut down the bank. You know, if the threat of the attack is big enough, yeah, you know, if you, if you're a small bank, and you get a Distributed Denial of Service, and you're very centralised, the entire bank could be offline. If your bank is purely digital, and you're only relying on a digital footprint, if someone brings down your customer-facing portals, as well as, your communication mechanisms, such as I don't know, WhatsApp chatbots, or IP telephones, you cannot operate."* (Participant JB15)

> *"So, we know ransomware is a massive issue. So, as you can imagine, you get different types of ransomwares, you get ransomware, that encrypts files, and you get ransomware. That encrypts, hard drives and systems. So immediately, if you if ransomware, enters an environment, and it starts encrypting files, encrypting systems, there's going to be an immediate and availability impact."* (Participant AA19)

One of the core principles of cybersecurity is the CIA triad, which is concerned with confidentiality, integrity, and the availability of resources. An attack on those three pillars adversely affects a bank's ability to render services securely and timeously to its clients. Material cyber-attacks could bring operations to a standstill. In 2019, when a DDoS attack targeted local banks, it disrupted online and mobile banking services.

Theme 2: Reputational damage: Participants indicated that the attacks could impact the banks' public image, which is a salient matter, as that could also affect other aspects of the banks. This was summarised by the participants, who stated:

> *"And then obviously, the big elephant in the room is the reputational damage that comes from that because, as you know, if your customer doesn't trust you anymore, your customer is 95% of the time going to go somewhere else."* (Participant AA19)

> *"Reputational damage reputation itself obviously is terrible, this type of attacks and the times will go out to the media, with people being shallow beings or they are they will, you know, think they think you want to move banks because you don't wanna you know, lose your money or being at a risk."* (Participant NM21)

> *"So, the implications could be catastrophic for the bank, you know, in a nutshell. And with that said, I think the manner in which the bank would respond to such attacks, if, let's say, a bank is breached, right, the manner in which they respond to that I take my either one leads to reputational damage, loss of revenue, loss of confidence from clients from their client base, you know, or on the opposite."* (Participant TM02)

Reputational damage and trade name devaluation are natural consequences of cyber-attacks. Trust between clients and investors is usually eroded when organisations are victims of cyber incidents. Hollard (2017), an insurance provider in South Africa, states how a cyber incident that occurred at Standard Bank South Africa, which cost the bank around ZAR 300 million, had an impact on the organisation's reputation, not only because of the attack but also because of the downtime associated with these attacks. Agrafiotis, Nurse, Goldsmith, Creese, and Upton (2018) identified reputational harm as a cyber-harm resulting from cyber-attacks. They stated that reputational harm adversely affects how the public perceives an organisation, which might, in turn, affect how the media portrays the organisation and the relationship between the organisation and its stakeholders.

Theme 3: Financial losses: Most participants identified financial impact as one of the foremost direct impacts of cyber-attacks and threats on commercial banks. It was also evident that participants knew that financial losses faced by commercial banks when dealing with cyber-attacks came not only from the cybercriminals carrying out attacks but also from the regulators who could impose fines on the banks for such material breaches. The responses of the participants often included phrases such as:

> *"I mean, quoting the words of our CEO, cyber threats have the potential to bankrupt the bank. And probably even make us shut down in a very short space of time."* (Participant KS12)

> *"There is a potential for financial losses, there is a potential for regulatory losses in terms of fines from the regulatory body when there is if it is determined that sufficient controls were not put in place to prevent the incident from happening"* (Participant OO04)

> *"If the bank were to be hacked, shame, God forbid, and your traders don't have access to the market, the bank would lose millions because then you won't be able to bid in the market like wouldn't be able to participate. Even I think even if they were to close us*

> *for a few hours, there'd be millions lost on the market. And that could result in the bank losing the share price, which would definitely drop."* (Participant VS18)

The participants' views were corroborated by an Accenture report (2019), which showed that the annual costs of all types of cyber-attacks are increasing, with the average price of an attack totalling US$ 13.0 million in 2018. Within South Africa, fines are imposed by the South African Reserve Bank and the Information Regulator, depending on the type of infringement. Examples of these fines include a ZAR 1 million on Habib Overseas Bank Limited for inadequate internal controls for detecting suspicious and unusual transactions. Investec Bank Limited was fined R20 million for a similar transgression (South African Reserve Bank, 2020). Recent examples of such fines include a possible penalty placed on the credit bureau TransUnion for a cyber breach that affected data belonging to South African citizens. The credit bureau faced a potential fine of ZAR 10 million for the violation (My Broadband, 2022).

Furthermore, Deloitte (2022) posited that the impact of cyber-attacks is often far more far-reaching than well-understood impacts such as regulatory fines, public relations costs, and breach notification and protection costs. They claimed that there are more hidden costs to cyber breaches that are often not visible to the public and potentially affect an organisation's bottom line for years. Some of these less-mentioned impacts that affect bottom lines are insurance premium increases, increased cost of raising debt, operational disruption or destruction effect, the value of lost contract revenues and the devaluation of their trade name, to name a few.

Theme 4: Loss of investor and customer confidence: The last subtheme that emerged from the participants was how suffering cyber-attacks could result in a financial institution losing investors and how customers' confidence in the institution might suffer. It was evident from the responses below that the participants were acutely aware of the devasting impact cyber-attacks would have on banks' market share because they are publicly traded companies.

Their views are supported by extensive literature that cites that the announcement of cybercrime often negatively impacts the market value of stock prices (Smith, Jones, Johnson, & Smith, 2019). Loss of investor confidence was not the only ramification an institution would suffer from because of a cyber-attack. Participants also expressed how the customers of the commercial banks could lose trust in the bank.

EY Global (2019) reaffirmed participants' views by stating that cyber-attacks can destroy trust between organisations and their customers. This is because, in recent times, customers have been providing more data to organisations. Concurrently, concerns around data privacy and cybersecurity have been growing among customers. The responses of the participants are quoted below:

> *"And shareholders would not have faith, you know, in the bank itself. Because if you're unable to protect your systems against cyber-attacks, then they cannot trust that the interests are protected in the bank, and they feel very vulnerable. So, you can do a lot in terms of the share price."* (Participant VS18)

> *"In terms of, you know, you could lose, number one, some very important information of your clients, which in turn will result in a loss of trust with the clients in the bank. And, you know, you could lose market share"* (Participant DM01)

> *"So, the implications could be catastrophic for the bank, you know, in a nutshell. And with that said, I think the manner in which the bank would respond to such attacks, if, let's say, a bank is breached, right, the manner in which they respond to that attack may either lead to reputational damage, loss of revenue, loss of confidence from client from their client base, you know, or on the opposite."* (Participant TM02)

5.3.9 Consideration Is Given to Cybersecurity Within Processes In The Bank.

The above question was asked for the researcher to understand whether cybersecurity was considered within processes in the organisation and whether they had encountered security within their domains when developing solutions.

Theme 1: Security is not considered because security is a siloed operation: The central theme that emerged from that question was that security was not considered at every stage of organisation processes because participants viewed security as a siloed operation within their organisation. This can be seen in their responses below. Some participants explicitly stated that security was an isolated department, and other statements showed that participants were only concerned with their personal work domain.

> *"I don't think so. I think they are isolated to the department that deals with the protection of the bank. So, I don't think they consider every aspect."* (Participant MR11)

> *"No. The reason is because of lots of siloed organisations and, again, bureaucracy."* (Participant JB15)

> *"No. Like, the reason why I say no is because, like, like I'm saying, I am a Java developer, for example. And as a Java developer, I'm so focused on the things that sort of, I need to get done. My, like, the whole silo thing."* (Participant SD17)

Security operating in a silo is one of the challenges Blum (2020) listed regarding cybersecurity. He posited that moving security from a silo to a more cross-functional operation would give cybersecurity leaders the resources and support structures they required to defend the organisation they served adequately. Albert (2020) mentioned how security had recently played an increasingly essential role in all parts of their business. Now more than ever, companies need to approach security holistically across all aspects of businesses, from people processes to continuity planning. Security is now everyone's responsibility, and it is a shared responsibility. IBM drove this point home by highlighting that inability to reduce silo and turf issues in IT significantly contributed to the stagnation of cyber resiliency in organisations (IBM, 2022).

Theme 2: No, because business requirements come first. The participants' responses below highlighted how businesses viewed security. Security is often seen as a deterrent to getting out features and solutions. From the view of the participants, it is evident that business requirements usually take precedence over security. Participants expressed how often there is a push from businesses to get products to market under specific time constraints and that, due to those constraints, information security officers often ignore security and look at the minimum requirements for their solutions to be compliant and ready for market. The responses that demonstrate this are shown below:

> *"I mean, I'm probably not innocent myself. But you know, most of the time, things like your projects, your, you know, the products that you want to get out on in the market, and the things are just rushed. And it's just the nature of how competitive the industry is. They are rushed to a point that you know, some things are missed. So, I don't think they're always missed."* (Participant NM21)

> *"No. Like, you know, when it comes to business, businesses business, and when it comes to cyber, cyber is cyber, right? The two, and as much as we've got information security officers, the information security officer will just look at whether we are compliant."* (Participant HN07)

> *"No. It doesn't. It doesn't. Business is trying to push features. And this is my experience, right? Until they get a pushback of approval somewhere. Right, that security needs to approve this. A lot of the times, that's when some features then consider security."* (Participant KS12)

From the responses above, it is evident that more needs to be done to leverage security within organisations' product and solution development. Security should not be seen as a blocker but rather as an enabler of producing secure products for clients and the organisation. In Rational

Cybersecurity for Business: The Security Leaders' Guide to Business, Blum (2020) stated that for organisations to achieve the promise of cybersecurity, leaders from both business and security need to align and rationalise cybersecurity. The myth that cybersecurity is just a technical problem needs to be dispelled, and rational cybersecurity needs to be adopted whereby an explicitly defined security programme based on risks, culture, and capabilities of an organisation that is supported by executives and is aligned with the mission of stakeholders and processes is adopted.

Theme 3: No, lack of awareness: A subtheme that emerged was that security was not considered at every stage of a process in organisations because the designers or implementors of the solutions were unaware of security or how to incorporate security into their process. The subtheme corresponds to similar themes identified in other organisations that participants posed. The participants highlighted that security within their organisations was siloed and that there was little interaction between ordinary users and security professionals.

> *"Yeah. I don't think that cybersecurity is taken into consideration at every step. No, there needs to be a lot more education and awareness."* (Participant JB15)
>
> *"No. I don't think they are, because if they were, then everyone, including myself in the bank, would know about cybersecurity, that, you know, interventions will just know the minimum, because right now we just need we need to we know."* (Participant VS18)

The above responses highlighted that there is still room for improvement in security awareness within organisations' development lifecycles of solutions. Security needs to be more tightly integrated with other parts of technology in organisations, and it should be seen as a partner seeking solutions and not just a deterrent to progress.

Theme 4: Yes, security is considered in the design phase: Few participants believed that security was considered within the design phase of products. Although not a vast majority of the participants were of this view, it was still enough to emerge as a subtheme from the question. Those with that view expressed that it was considered because risk had to be considered when developing solutions. Their responses are below:

> *"Definitely they are. I mean, in every project that I've been in, we will always consider the risk factor."* (Participant RG13)
>
> *"Yeah, I think so. I think so. I think, you know, to my previous point, you know, maybe we don't maybe the banking institutions don't understand themselves fully, maybe they don't understand the threat, the threats and the threat actors fully, but they're the efforts*

> *to ensure that every single piece of the puzzle does not move without security oversight is something that I have found to be working effectively"* (Participant MN14)

> *"Definitely, they are because in each and every audit that me that I am or that we are doing or involved with, we do consider IT risk security information"* (Participant NT03)

Various approaches exist to developing solutions and software that put security and privacy at the forefront of developing solutions. These novel approaches to developing information system solutions have been driven by the progress made by attackers and the continuously evolving threat landscape regarding application security (Baldassarre, Barletta, Caivano, & Scalera, 2020). Privacy by design is such an approach. It seeks to proactively embed privacy into the design and operation of IT systems, networked infrastructure, and business practices. One of the benefits of such an approach, as mentioned by Deloitte (2022), is that privacy by design promotes avoiding legal liability, thereby maintaining regulatory compliance and brand protection and preserving customer confidence. Other approaches to solution development that see security being incorporated earlier in the process are security by design, secure software development, and secure architecture.

5.4 Chapter Summary

This chapter commenced with a short restatement of the data collection process for the study, followed by a brief description of the thematic data analysis process to identify the themes in each of the questions posed to the participants. A presentation of the participants' demographic details followed. Right after that, a presentation of each interview question was tabled. The findings around each interview question were presented and discussed based on the literature and participants' opinions. The next chapter seeks to analyse and present the conclusions of the quantitative data collection of the study to establish whether the findings from qualitative and quantitative are aligned and reinforce any conclusions of either form of data collection.

Chapter Six : Presentation And Discussion Of Quantitative Findings

6.1 Introduction

This chapter presents and discusses the study's quantitative findings according to the research procedures outlined in chapter four. Quantitative data was collected from professionals within IT, Risk, Audit, Compliance, and other varied professions within the banking domain in South Africa. The data was collected using a survey over thirteen months, from March 2021 until April 2022. The structure of the chapter is similar to the previous chapter. The first section discusses the demographic profile of the respondents, and the second section focuses on the data analysis using multivariate analysis. As part of the multivariate analysis, descriptive statistics for each survey question are presented. The descriptive statistics mainly focus on the mode of the responses and the median. CFA was also applied to the collected data set to create a model to identify the relationships between the identified factors. Lastly, the chapter discusses the findings from the analysis and summarises the chapter.

6.2 Demographic Profiles Of Respondents

A total of two hundred and forty-three respondents completed the survey. From that number, only two hundred and twenty-nine were used for the study. The number of respondents was less than the stated sample size of three hundred and eighty-four. This could be attributed to the researcher's challenges with data collection during the survey. However, significant effort was employed to meet the sample size. The researcher observed that identified respondents were often reluctant to complete the study, fearing it would violate their organisation's stance on clicking on unsolicited links. Furthermore, some respondents indicated in the demographic section that they did not work for commercial banks but completed the survey. Removing the fourteen invalid entries from the data was done manually by going through each response to see where the respondent was employed and whether their position made them valid for the study. The participants' demographic profiles were varied and encompassed all but a handful of commercial banks in South Africa. Two relatively new digital commercial banks were not represented in the survey data, although the researcher attempted to get respondents from those new commercial banks to participate in their place. The following subsections discuss the demographic distribution of the respondents in great detail.

6.2.1 Gender

Ninety-two females, one hundred thirty-five males, and two respondents who chose not to reveal their gender completed the survey. The distribution of genders was such that females made up 40.2 per cent of the respondents. Males made up 59 per cent and those who chose not to reveal their gender made up 0.8 per cent. Figure 6.1 depicts the distribution of genders among the participants. As Bert (2018) stated, gender diversity in a scientific research study provides a unique perspective to research from all genders. It also helps form a better generalisation of the population.

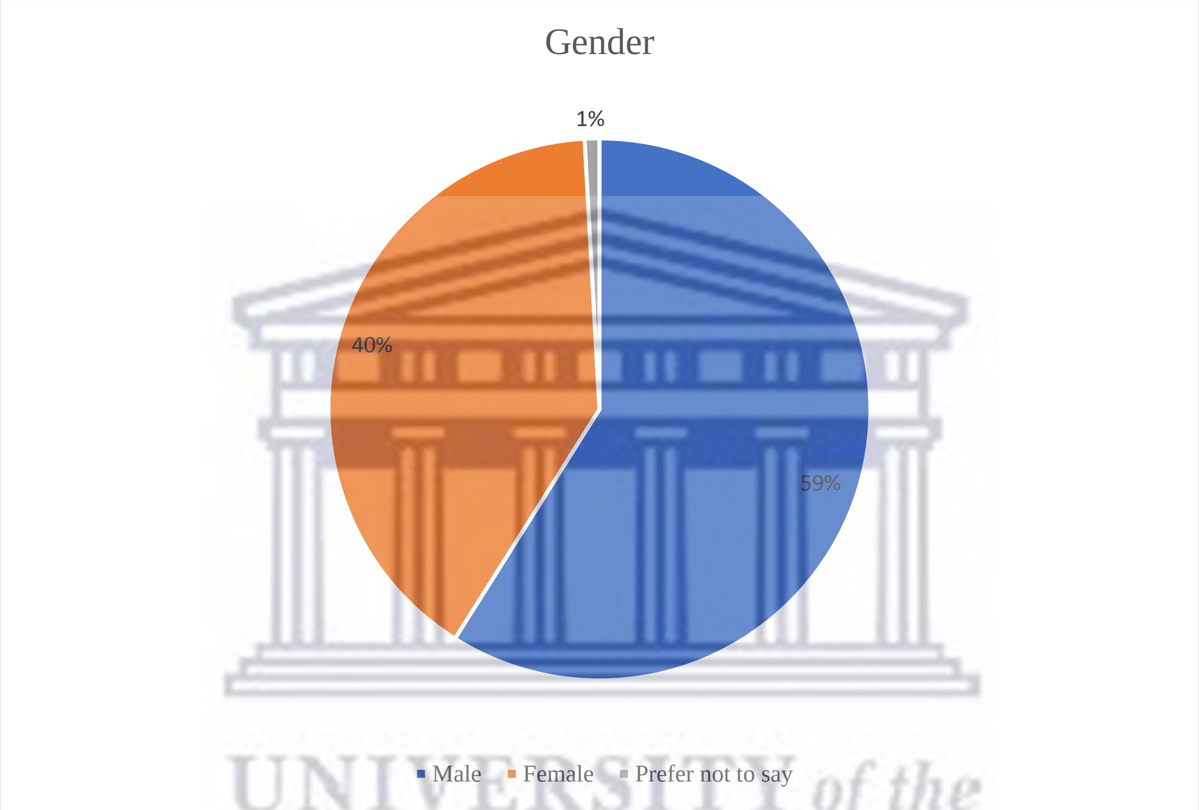
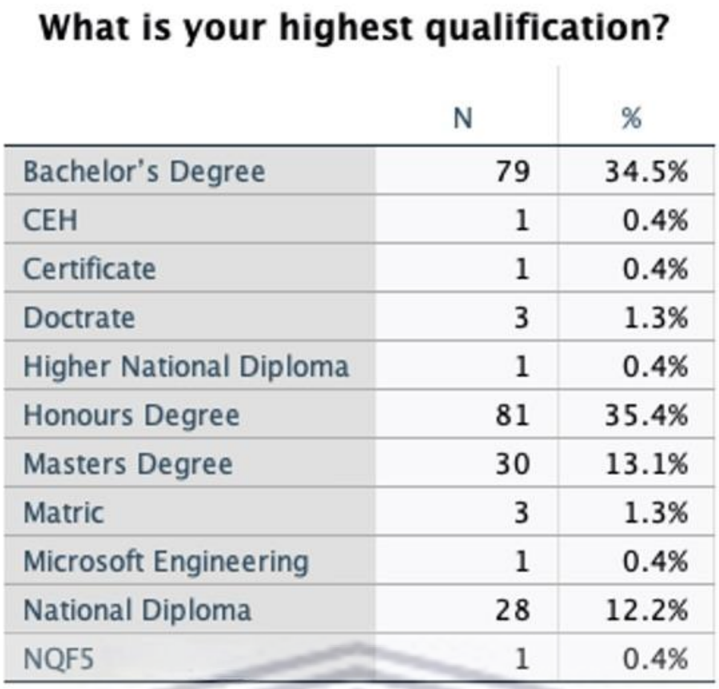


Figure 6.1 Gender distribution

6.2.2 Highest Qualification

The survey respondents held eleven qualifications. The majority (35.4 per cent) of the respondents had an honours degree in their profession, followed closely by 34.5 per cent of respondents with a bachelor's degree. Table 6.1 shows an in-depth distribution of the rest of the qualifications held by the respondents. The results show that all the respondents held formal education qualifications that made them relevant to the study, and those who did not have certifications in the field of IT were still deemed suitable for the study.

Table 6.1 Distribution of qualifications



What is your highest qualification?

	N	%
Bachelor's Degree	79	34.5%
CEH	1	0.4%
Certificate	1	0.4%
Doctrate	3	1.3%
Higher National Diploma	1	0.4%
Honours Degree	81	35.4%
Masters Degree	30	13.1%
Matric	3	1.3%
Microsoft Engineering	1	0.4%
National Diploma	28	12.2%
NQF5	1	0.4%

6.2.3 Age Group

Diversity in age offered varied perspectives from respondents on the matters at hand. For the survey, five age groups were created; the groups were 18-25, 26-35, 36-45, 46-55 and 56 years and above. Most of the respondents to the survey were in the 26-35 age group, which made up 73.80 per cent, followed by those in the 18-25 age group, which made up 18.78 per cent. Figure 6.2 shows the age distribution of the respondents.

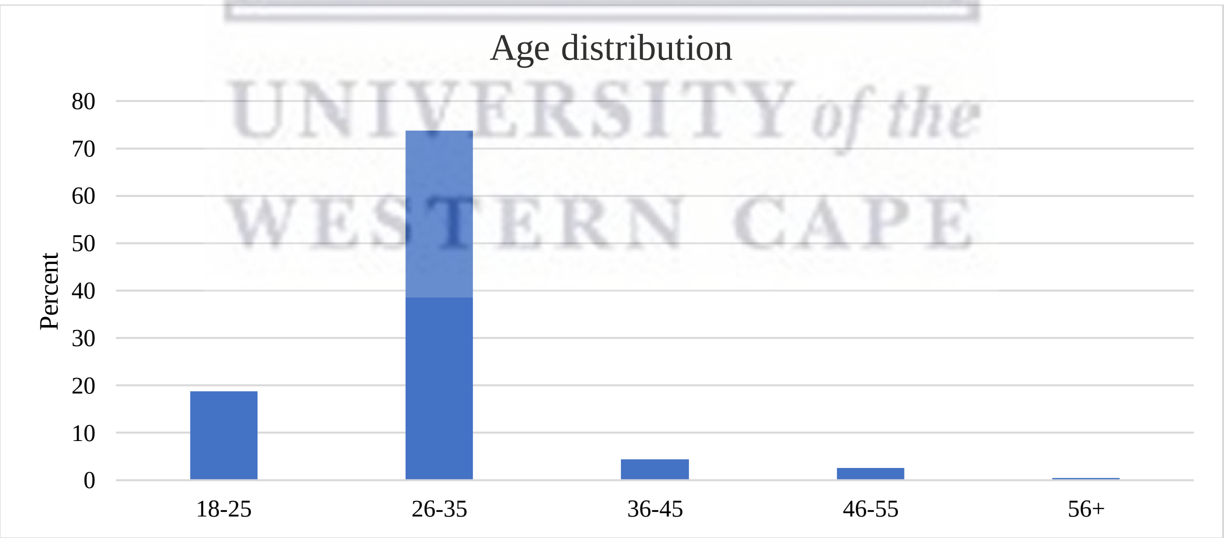


Figure 6.2 Age distribution

6.2.4 Years Of Experience

The bulk of the respondents to the study had working experience of between one and five years. These respondents comprised 43 per cent of the total respondents, followed closely by those with six to ten years of experience, contributing 27 per cent to the total number of respondents. The varied spread of respondents in terms of working experience gave a general picture of how cybersecurity was viewed across the board by those new to the working world and those with years of experience. The distribution of the respondents' working years is shown in Figure 6.3 below.

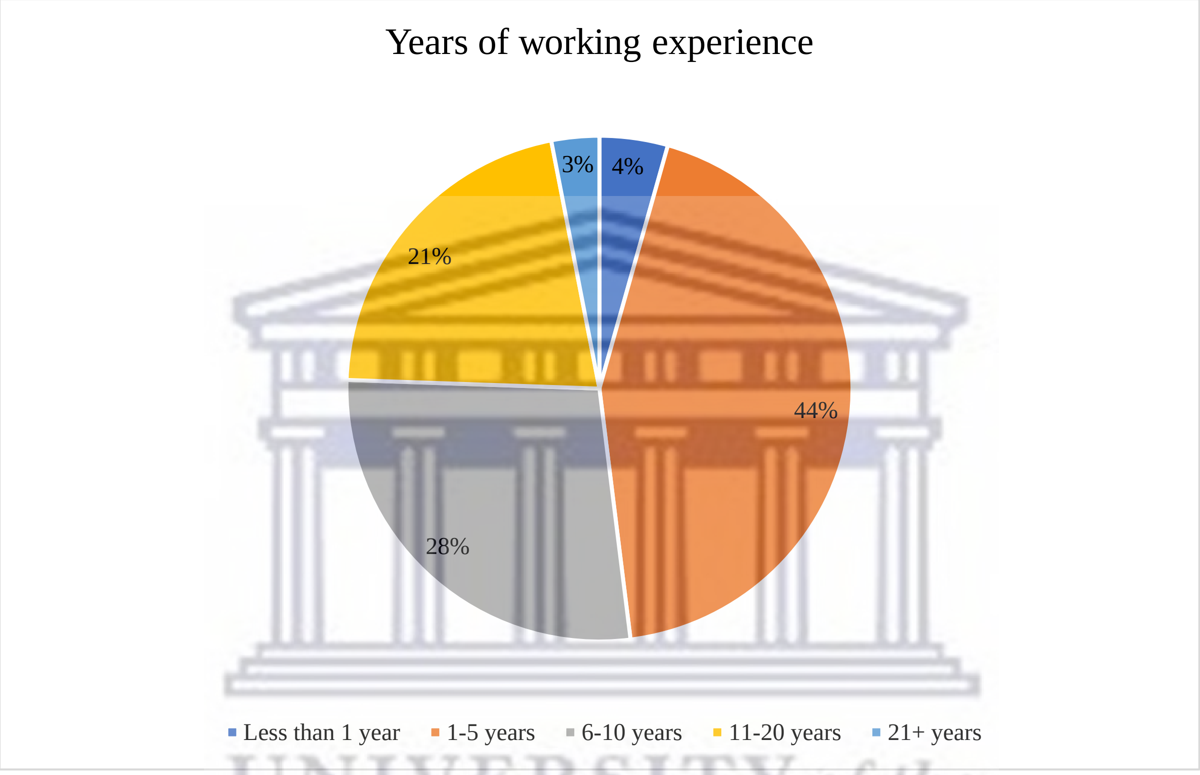


Figure 6.3 Workings years of respondents

6.2.5 Respondent Job Titles

Diversity within the job titles held by respondents proved valuable in generalising the views held by technical employees within the banking landscape of South Africa. It also offered varied responses by gathering data from those with in-depth knowledge of cybersecurity, as opposed to those who were not cybersecurity experts but still found themselves within commercial banks' technology, risk, or governance spaces. The survey represented seventy-one job titles, varying from management titles to interns who had just started working, with the most prominent title being DevOps Engineer. Figure 6.4 shows the various job titles held by the respondents.

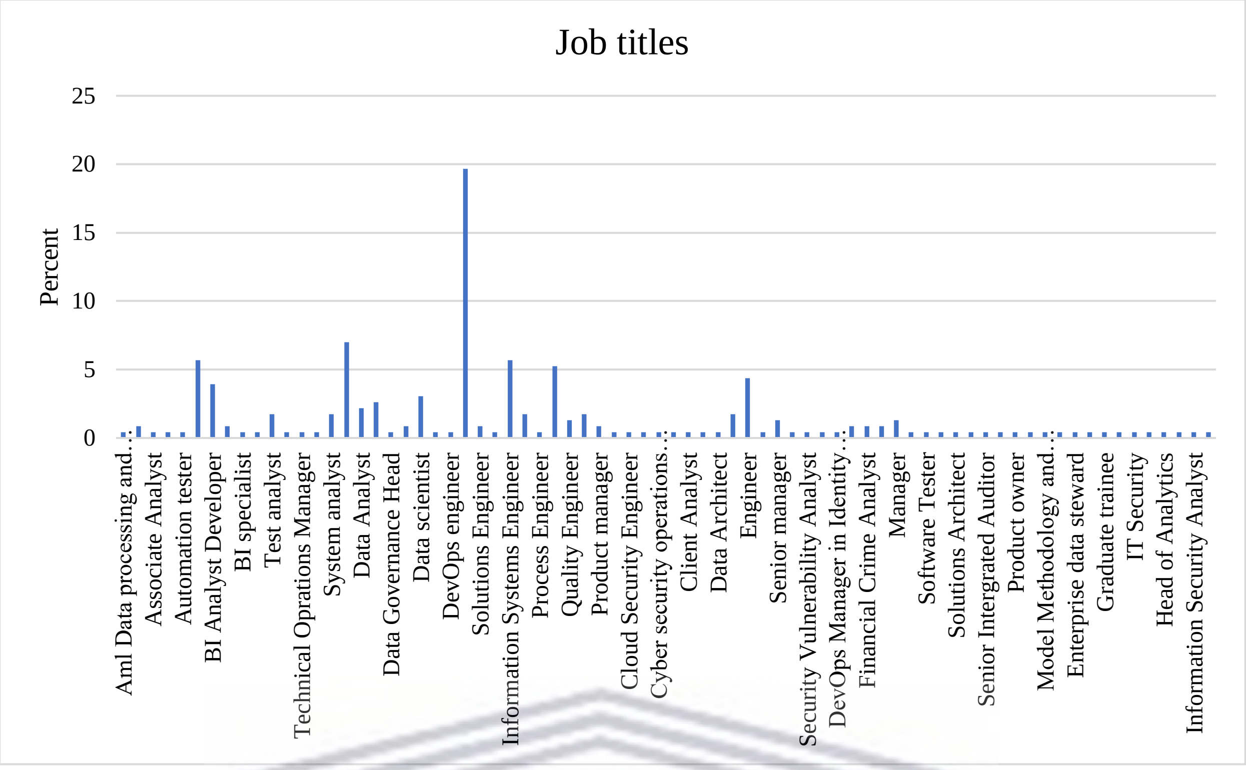


Figure 6.4 Respondent job titles

6.2.6 Employers

The respondents were distributed across fifteen commercial banks in South Africa. There is a possibility of more than fifteen commercial banks in the study because some respondents filled in their employer as ‘Other’ instead of naming them. Figure 6.5 summarises the distribution of employers from the respondents. For anonymity, the names of the banks have been replaced with arbitrary alphabet letters that are not associated with banks.

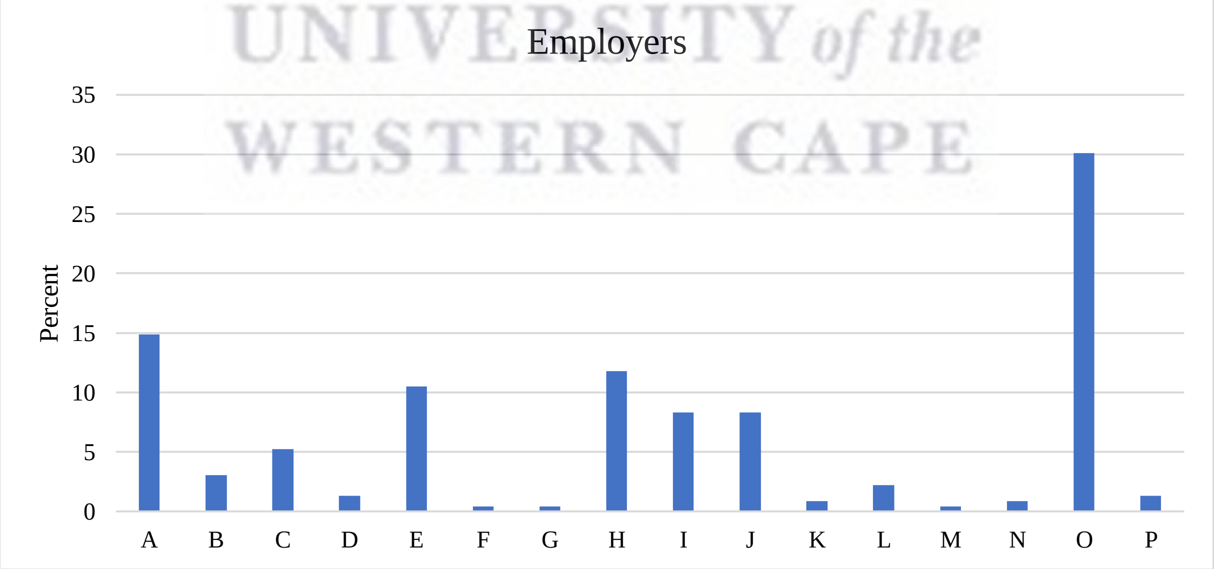


Figure 6.5 Distribution of employers

6.3 Reliability Tests

To ensure internal consistency, a measure of reliability was used, described by Revicki (2014) as a measure that reflects the extent to which grouped items within an instrument measure various aspects of the same characteristic or construct. The Cronbach Alpha test was employed to measure the internal consistency of grouped Likert items that measured a single variable. Cronbach's Alpha is a test used to calculate the internal consistency of a test or scale. It is between 0 and 1.0 (Tavakol & Dennick, 2011). The closer the value is to 1.0, the greater the internal consistency of the items under consideration. Values between .70 and .99 are generally accepted as reliable (Mohamad, Sulaiman, Sern, & Salleh, 2015). The initial Cronbach Alpha coefficient results indicated internal consistency for the variables that measured security awareness, the influence of human behaviour on cybersecurity, threat awareness, and the impact cyber-attacks and threats have on commercial banks. The variables that measured security posture and training did not achieve internal consistency within an acceptable range, as shown in Table 6.3. However, to remedy the lack of internal consistency, the suggestion made by SPSS to remove specific items was adopted. After removing those items, the variables achieved an internal consistency within acceptable ranges, as seen in Table 6.4. Table 6.2 is a legend that describes the variables used.

Table 6.2 Variable Legend

Variable	*Acronym*
Human behaviour	HB
Security Awareness	SA
Security Posture	SP
Security Training	ST
Threat Awareness	TA

Cronbach Alpha results.

Table 6.3 Variables without internal consistency

Variable	*Cronbach's Alpha*	*Cronbach's Alpha Based on Standardised Items*	*Number of Items*
SP	.674	.709	6
ST	.529	.552	3

Table 6.4 Cronbach Alpha results

Variable	***Cronbach's Alpha***	***Cronbach's Alpha Based on Standardised Items***	***Number of Items***
HB	.815	.816	2
ST	.814	.814	2
TA	.839	.842	3
SA	.716	.717	2
SP	.752	.765	5

6.4 Descriptive Analysis

The following section provides a descriptive analysis of the findings. Each of the sixteen Likert items will be presented and discussed. Descriptive statistics summarises the characteristics and distribution of the values in one or more datasets. It allows researchers to quickly explore the central tendency and the degree of dispersion of the values in the dataset (Lee, 2020).

6.4.1 I know how human behaviour affects Cybersecurity in the institution.

The literature showed that humans are one of the weakest links within the cybersecurity chain. Zimmermann and Renaud (2019) stated that they had found that humans were generally identified as the most significant problem within cybersecurity. Most respondents (103), which comprised 45 per cent of the total respondents, indicated “Strongly Agree” with the statement posed, while 35.4 per cent “Agreed” with the statement. Awareness of cybersecurity and the impact an individual has on organisations' overall security posture was one of the challenges identified by ENISA (2021). This agreed with (Marble *et al.*, 2015), who stated that the human element was the common thread among all cyber threats. Figure 6.6 depicts the responses collected from the respondents and indicates how most agreed that they knew the effect human behaviour had on cybersecurity, as shown in Table 6.5 Effect of human behaviour.

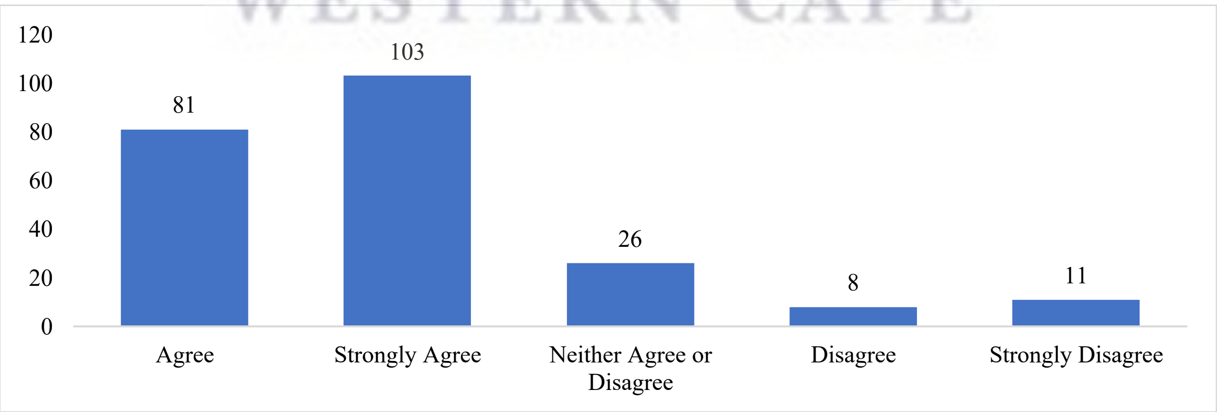


Figure 6.6 Effect of human behaviour

I know how human behaviour affects cybersecurity within the institution.				
		Frequency	Per cent	Valid Per cent
Valid	Agree	81	35.4	35.4
	Strongly Agree	103	45.0	45.0
	Neither Agree nor Disagree	26	11.4	11.4
	Disagree	8	3.5	3.5
	Strongly Disagree	11	4.8	4.8
	Total	229	100.0	100.0
Median		Agree		
Mode		Strongly Agree		

Table 6.5 Effect of human behaviour

6.4.2 Human Behaviour Greatly Affects Cybersecurity Within The Institution.

Like the previous statement posed to respondents, this statement investigated whether respondents knew how human behaviour affected the institution's security because any cybersecurity framework within an institution must consider the cybersecurity culture within the institution and the societal context within which it operates (Jeong, Oliver, Kang, Creese, & Thomas, 2021). Figure 6.7 and Table 6.6 Human behaviour

show that an overwhelming majority (86.9 per cent) of the respondents either "Strongly Agreed" or "Agreed" with the statement. In comparison, only a few (6.1 per cent) of the respondents did not agree with the statement. The responses align with the literature that showed that human behaviour and, to a greater extent, cybersecurity culture play a significant role in upholding the security posture of an institution. Keman and Pearlson (2019) proposed that building a good cybersecurity culture within an organisation influences employee behaviour and ultimately increases the organisation's cyber resilience.

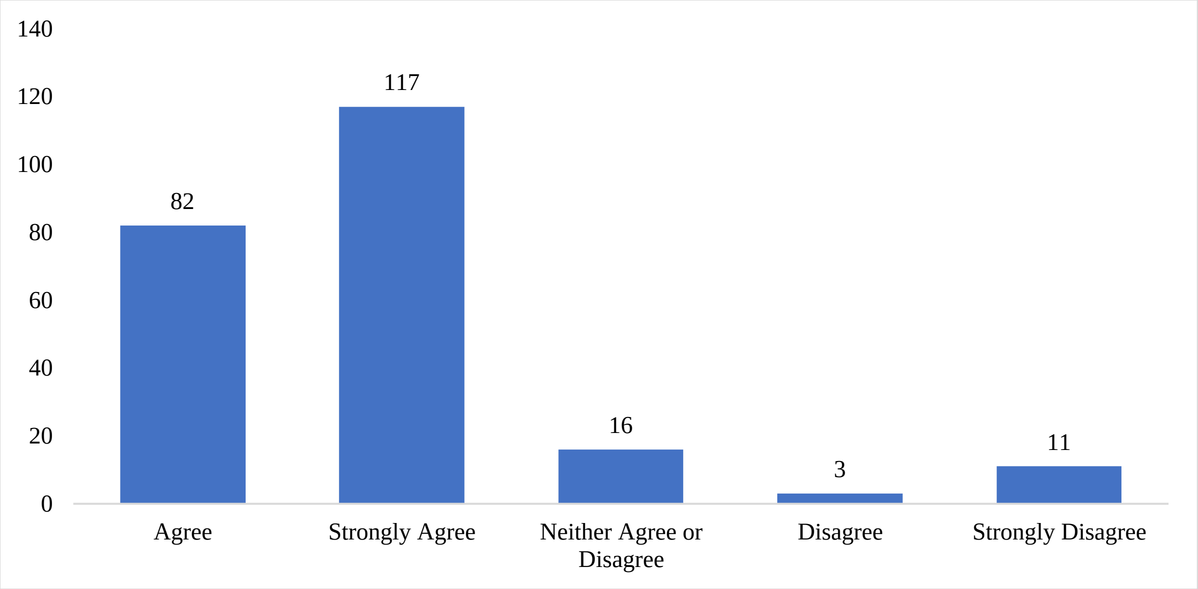


Figure 6.7 Human behaviour

Human behaviour significantly affects cybersecurity within the institution.				
		Frequency	Per cent	Valid Per cent
Valid	Agree	82	35.8	35.8
	Strongly Agree	117	51.1	51.1
	Neither Agree nor Disagree	16	7.0	7.0
	Disagree	3	1.3	1.3
	Strongly Disagree	11	4.8	4.8
	Total	229	100.0	100.0
Median		Strongly Agree		
Mode		Strongly Agree		

Table 6.6 Human behaviour

6.4.3 I follow all the rules and regulations outlined in the security guidelines

This question aimed to gauge the respondent's adherence to the rules and regulations laid out by commercial banks concerning security. This is because adherence to cybersecurity guidelines and practices was seen as a critical pillar to maintaining a good security posture within organisations. Failure to adhere to guidelines often weakens an organisation’s security posture (Davis & Olson, 1985; Karlsson *et al.*, 2017). From the findings in Figure 6.8, it is evident that most respondents adhered to the guidelines set out by their organisations. This was evidenced by 82.5 per cent of the respondents either strongly agreeing or agreeing to adhere to the guidelines. The results from the two previous findings supported the results in this finding because, as stated by Siponen, Mahmood, and Pahnila (2014), some of the factors that drive compliance with information security policies and regulations are attitudes towards compliance awareness presented in security education and hands-on training and social norms.

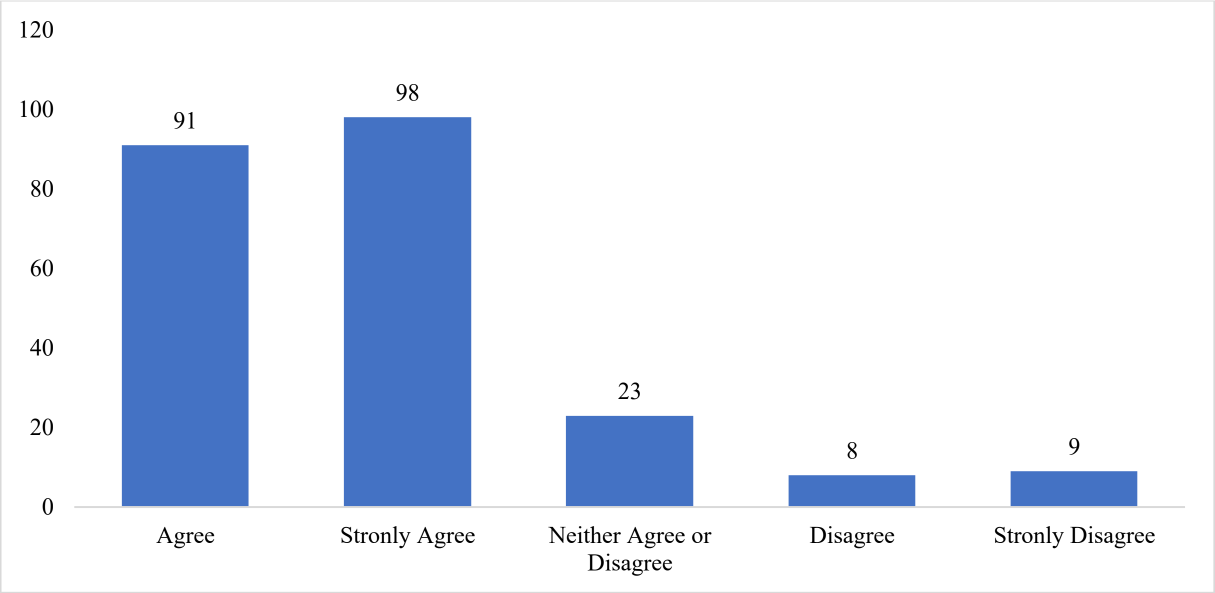


Figure 6.8 Adherence to guidelines

I follow all the rules and regulations outlined in the security guidelines.				
		Frequency	Per cent	Valid Per cent
Valid	Agree	91	39.7	39.7
	Strongly Agree	98	42.8	42.8
	Neither Agree nor Disagree	23	10.0	10.0
	Disagree	8	3.5	3.5
	Strongly Disagree	9	3.9	3.9
	Total	229	100.0	100.0
Median		Agree		
Mode		Strongly Agree		

Table 6.7 Adherence to guidelines

6.4.4 Rules Such As Bring Your Own Device Make It Easier For The Institution To Protect Its Assets

Bring your own device (BYOD) poses a risk to the security posture of an institution because organisations usually cannot enforce proper security measures on devices as they do not belong to the organisation. Often, group policy objects cannot be applied to the devices as they are usually not fully integrated into the organisation's domain. Most respondents indicated that they knew the challenges BYOD posed to institutions. Chigada and Daniels (2021) supported the respondent's views by stating that although BYOD was financially beneficial to organisations, it posed a significant risk if their use was not regulated and monitored within the organisation's network. Given how lenient security controls usually are on devices, they also act as a possible threat vector for attackers to exploit. This was shown by 32.8 per cent of the respondents disagreeing with the statement and 33.6 per cent strongly disagreeing that BYOD made it easier for institutions to protect their assets.

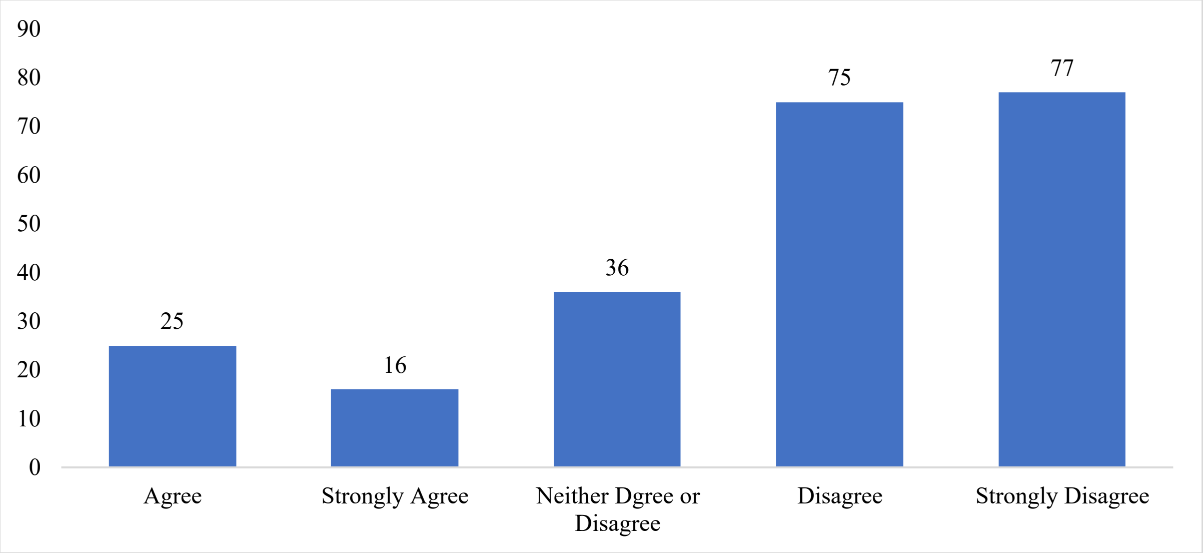


Figure 6.9 BYOD rules

Rules such as bringing your own device make it easier for the institution to protect its assets.				
		Frequency	Per cent	Valid Per cent
Valid	Agree	25	10.9	10.9
	Strongly Agree	16	7.0	7.0
	Neither Agree nor Disagree	36	15.7	15.7
	Disagree	75	32.8	32.8
	Strongly Disagree	77	33.6	33.6
	Total	229	100.0	100.0
Median		Disagree		
Mode		Strongly Disagree		

Table 6.8 BYOD rules

6.4.5 I am prepared to circumvent the cybersecurity protocols in place to get my job done.

The question above sought to understand the respondents’ likelihood of disregarding security guidelines and protocols to deliver their tasks within the work environment. With the shift to hybrid working models due to the COVID-19 pandemic, organisations had to tighten their assets' security measures, leading to more stringent controls that employees might have found restrictive. Newman (2017) and Deloitte (2021) stated that balancing security controls and not affecting employee productivity is essential. Employees might sometimes subvert the rules to complete their daily tasks or stop working due to the controls. However, most respondents (53.2 per cent) to this question stated that they would not circumvent the controls to complete their tasks. A considerable number of respondents (27 per cent) were prepared to circumvent the rules, while 19.7 per cent were undecided on whether they would circumvent them. The findings align with Pfleeger and Caputo (2012), who stated that employees may ignore or subvert the security controls when security interferes with tasks. Figure 6.10 shows the distribution of the responses captured.

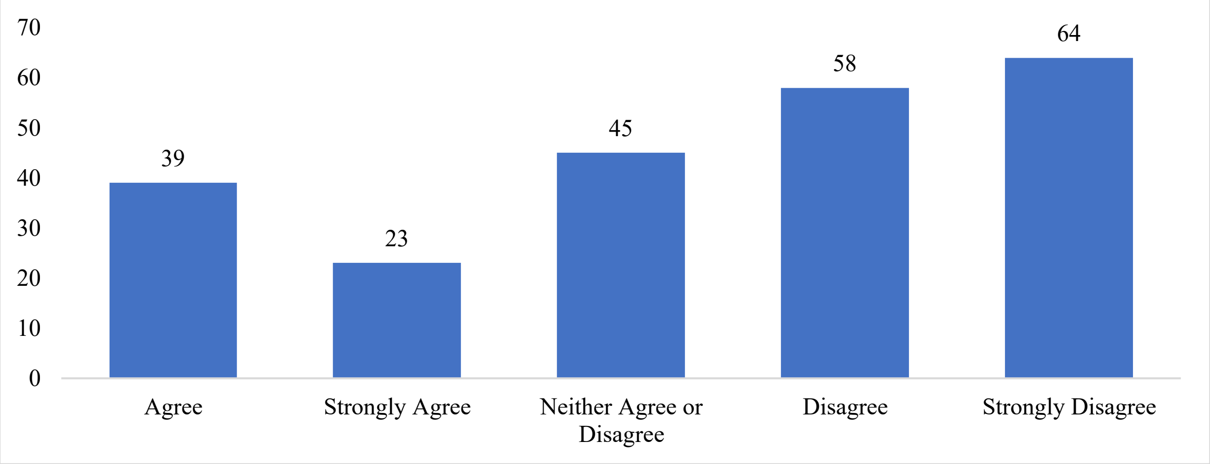


Figure 6.10 Likelihood to circumvent rules.

I am prepared to circumvent the cybersecurity protocols in place to get my job done.				
		Frequency	Per cent	Valid Per cent
Valid	Agree	39	17.0	17.0
	Strongly Agree	23	10.0	10.0
	Neither Agree nor Disagree	45	19.7	19.7
	Disagree	58	25.3	25.3
	Strongly Disagree	64	27.9	27.9
	Total	229	100.0	100.0
Median		Disagree		
Mode		Strongly Disagree		

Table 6.9 Likelihood to circumvent rules.

6.4.6 The Institution Has Imposed Some Cybersecurity Protocols That Make It Difficult for me to Do My Job

Similar to the previous question, this question was intended to gauge how respondents felt about the security controls put in place by organisations. The overall intention of this question was to measure whether respondents thought that the controls in place restricted their ability to complete their tasks and, if they felt that way, how likely they were to circumvent the controls in place to complete their assignments. Figure 6.11 shows that an overwhelming number (54 per cent) of participants felt that the controls did not restrict their ability to deliver tasks. However, 19.2 per cent of the respondents indicated that the controls hampered their ability to do their jobs. In comparison, 26.6 per cent of the respondents were unsure about the impact of security controls on their ability to deliver work. Lennartsson, Kävrestad and Nohlberg (2021) stated that users rejected unusable solutions whenever security conditions were too high. A balance must be established between security and usability, with management careful not to overwhelm users with overly complex systems.

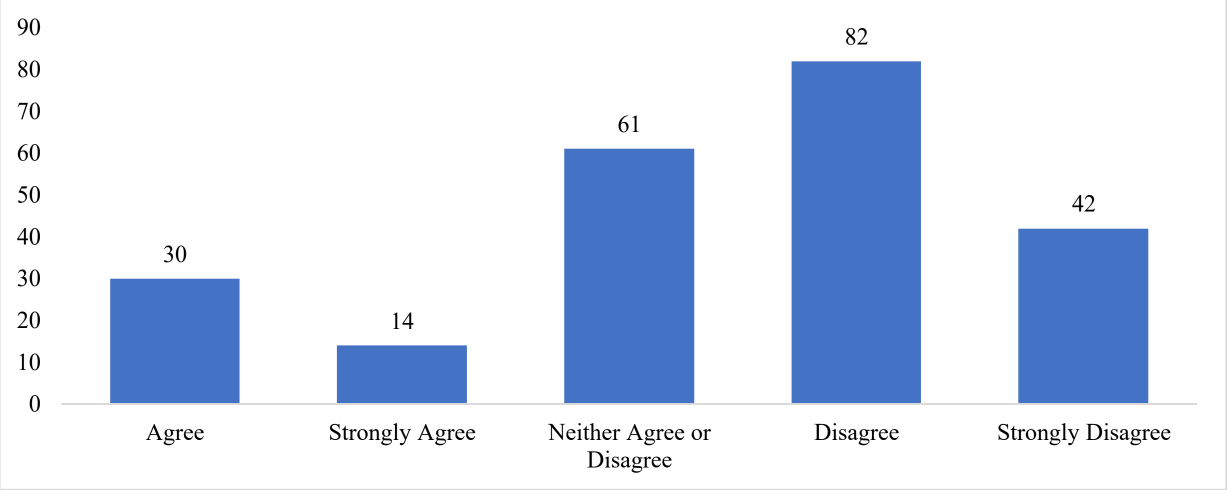


Figure 6.11 Imposed security controls.

The institution has imposed some cybersecurity protocols that make it difficult for me to do my job.				
		Frequency	Per cent	Valid Per cent
Valid	Agree	30	13.1	13.1
	Strongly Agree	14	6.1	6.1
	Neither Agree nor Disagree	61	26.6	26.6
	Disagree	82	35.8	35.8
	Strongly Disagree	42	18.3	18.3
	Total	229	100.0	100.0
Median		Disagree		
Mode		Disagree		

Table 6.10 Imposed security controls.

6.4.7 I trust the cybersecurity protocols to identify, protect, detect, respond, and recover from cybersecurity threats

Blum (2020) stated that incident response capabilities are critical to a successful security programme within organisations. They enable organisations to look at their entire digital estate and understand the activities within the estate and their ability to respond to cybersecurity incidents should they occur. That question was intended to assess the level of trust respondents had in their institution's incident response capabilities and continuous cybersecurity monitoring. Figure 6.12 shows that 83 per cent of the respondents had trust in the incident response capabilities of the organisations. In comparison, only 7.4 per cent of the respondents did not believe their institution had adequate incident response capabilities. Gcaza and Von Solms (2017) posited that trust was essential in cultivating a cybersecurity culture and that a lack of trust among parties in an organisation leads to a compromised security posture.

Aldawood and Skinner (2018) further supported the sentiment that trust is vital to upholding an organisation's security posture by stating that trust is critical in every aspect of an information security system and might affect employees' security conduct.

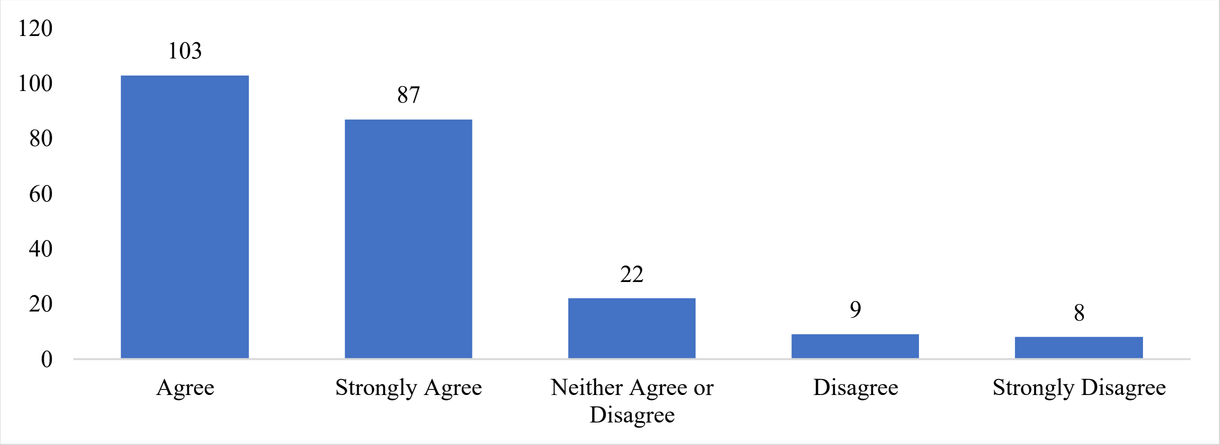


Figure 6.12 Incident response capabilities

I trust the cybersecurity protocols to identify, protect, detect, respond, and recover from cybersecurity threats.				
		Frequency	Per cent	Valid Per cent
Valid	Agree	103	45.0	45.0
	Strongly Agree	87	38.0	38.0
	Neither Agree nor Disagree	22	9.6	9.6
	Disagree	9	3.9	3.9
	Strongly Disagree	8	3.5	3.5
	Total	229	100.0	100.0
Median		Agree		
Mode		Agree		

Table 6.11 Incident response capabilities

6.4.8 I know my cybersecurity responsibility within the institution.

The World Economic Forum (2019) stated that cybersecurity in business is everyone's responsibility, not only those who are security experts. As part of that, everyone within a company should know which slice of the cybersecurity pie belongs to them. This statement was intended to determine whether respondents knew their role in upholding their institutions' security posture. Simultaneously, it sought to investigate whether the respondents had enough cybersecurity awareness. The responses in Figure 6.13 showed that most respondents knew their responsibility regarding upholding a secure cybersecurity posture because 46.3% of the respondents "Strongly Agreed" with the statement, and 38.4 per cent "Agreed" with the statement. Conversely, only 3.9 per cent of the respondents did not know their responsibilities within the institution, while only 9.6 per cent were undecided about their responsibilities. The findings align with the World Economic Forum’s view that cybersecurity is everyone’s responsibility within organisations. This was demonstrated by the overwhelming majority (84.7 per cent) of respondents who either “Strongly Agreed” or “Agreed” to know their cybersecurity responsibility within their organisation.

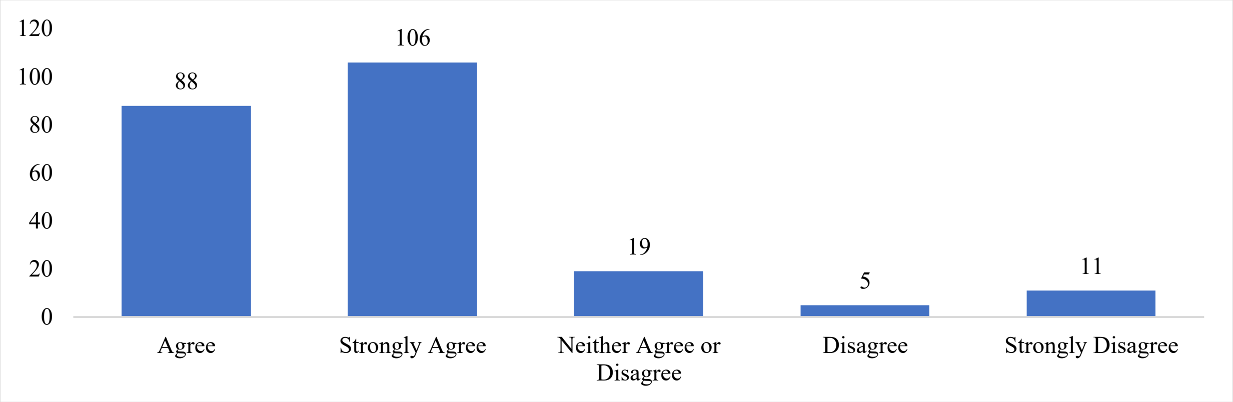


Figure 6.13 Cybersecurity responsibility

I know my cybersecurity responsibility within the institution.				
		Frequency	Per cent	Valid Per cent
Valid	Agree	88	38.4	38.4
	Strongly Agree	106	46.3	46.3
	Neither Agree nor Disagree	19	8.3	8.3
	Disagree	5	2.2	2.2
	Strongly Disagree	11	4.8	4.8
	Total	229	100.0	100.0
Median		Agree		
Mode		Strongly Agree		

Table 6.12 Cybersecurity responsibility

6.4.9 If A Cybersecurity Incident Occurs, I Know the Steps Needed To Report And Contain the Incident

The responses in Figure 6.13 showed that most respondents were aware of the steps they should take should they suspect that their systems had been compromised or that they were the target of a cybersecurity attack. 42.8 per cent of the respondents “Strongly Agreed” with the statement, while 34.5 per cent “Agreed” with the statement. Only a few (10.4 per cent) indicated that they did not know the steps for reporting a cyber incident within their institutions. This knowledge is essential for upholding a secure security posture and aiding incident response capabilities within institutions, as it allows the security teams to contain and remediate attacks quickly. The findings correlate with the earlier findings on participants’ cybersecurity responsibility within organisations because the effectiveness of SETA is usually measured by a decrease in the rate of clicking on malicious links, as well as the number of reported incidents to cyber incident response teams within organisations (Kwak, Damiano, & Vishwanath, 2020). SANS (2021) further supported the findings by stating that when users within an organisation are well-educated and informed about security risks, the time it takes to detect successful cyber-attacks decreases because users can quickly identify and report security incidents.

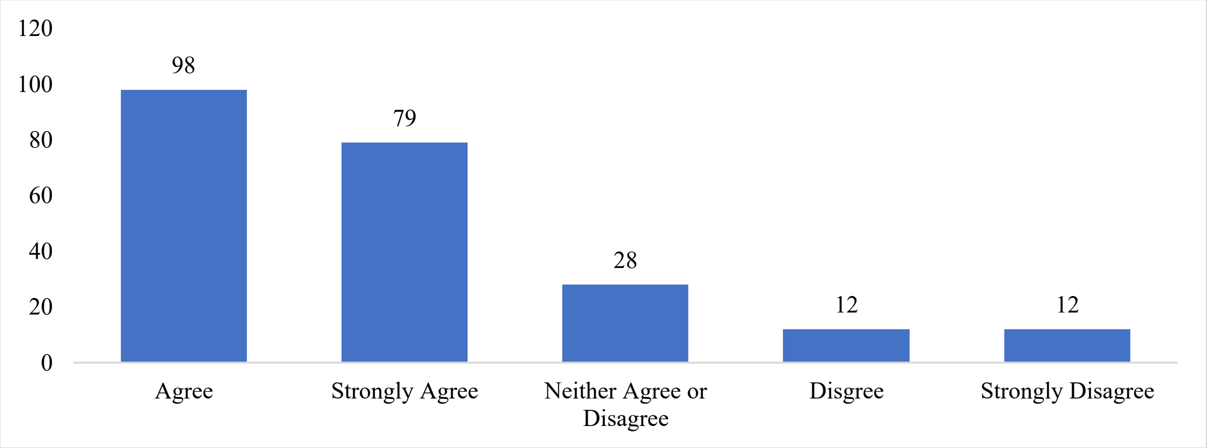


Figure 6.14 Reporting incidents

If a cybersecurity incident occurs, I know the steps needed to report and contain the incident.				
		Frequency	Per cent	Valid Per cent
Valid	Agree	98	42.8	42.8
	Strongly Agree	79	34.5	34.5
	Neither Agree nor Disagree	28	12.2	12.2
	Disagree	12	5.2	5.2
	Strongly Disagree	12	5.2	5.2
	Total	229	100.0	100.0
Median		Agree		
Mode		Agree		

Table 6.13 Reporting incidents

6.4.10 The Development of An Effective Security Framework Is Critical.

The NIST (2018) posited that one of the benefits of adopting or creating a cybersecurity framework is that a framework establishes a common language and a systematic methodology for managing cybersecurity risk. Frameworks also assist institutions in identifying their risks and charting a way forward to address them so that all the relevant stakeholders understand—the respondents' responses aligned with the views in the literature. Dimensional Research (2016) found that 84 per cent of the respondents in their survey supported a security framework within their organisation with the view that the framework guided security. Furthermore, Srinivas, Das and Kumar (2019) stated that a security framework provides security standards that each department within an organisation is supposed to achieve. Adopting a clearly defined security framework helps organisations improve security and adopt a positive security attitude. The sentiments were shared by an overwhelming number of participants, with (70.3 per cent) strongly agreeing with the statement and an additional 21 per cent agreeing with it. Cumulatively, only 5.7 per cent of the respondents did not agree with the criticality of developing a security framework, with a further 3.1 per cent being undecided. The distribution of the responses can be seen in Figure 6.15.

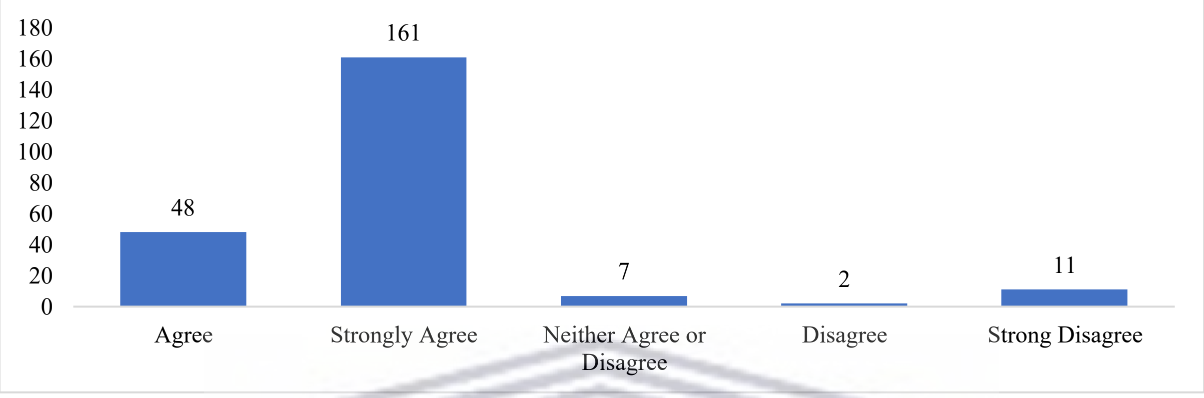


Figure 6.15 Criticality of a security framework

The development of a practical security framework is critical.				
		Frequency	Per cent	Valid Per cent
Valid	Agree	48	21.0	21.0
	Strongly Agree	161	70.3	70.3
	Neither Agree nor Disagree	7	3.1	3.1
	Disagree	2	.9	.9
	Strong Disagree	11	4.8	4.8
	Total	229	100.0	100.0
Median		Strongly Agree		
Mode		Strongly Agree		

Table 6.14 Criticality of a security framework

6.4.11 I know where to access the cybersecurity guidelines for the institution

Similarly to the other questions above, this statement sought to investigate the respondent's security awareness within their respective institutions, particularly concerning access to relevant information and documentation about cybersecurity. Access to information on how to protect oneself and uphold the institution's security posture is one way whereby institutions can defend themselves. According to Bahl, Sharma and Asghar (2021), the impact and the threat of cyber-attacks can be minimised through awareness campaigns. Hwang, Wakefield, Kim and Kim (2019) stated that security policies should be accompanied by visibility to be effective and that a lack of visibility around security often leads to less compliance. Figure 6.16

shows that 69.4 per cent of the respondents knew where to access the guidelines within their institution, which is representative of effective awareness about security. In comparison, only 16.6 per cent did not know, closely followed by 14 per cent of the respondents who were unsure about their access to guidelines.

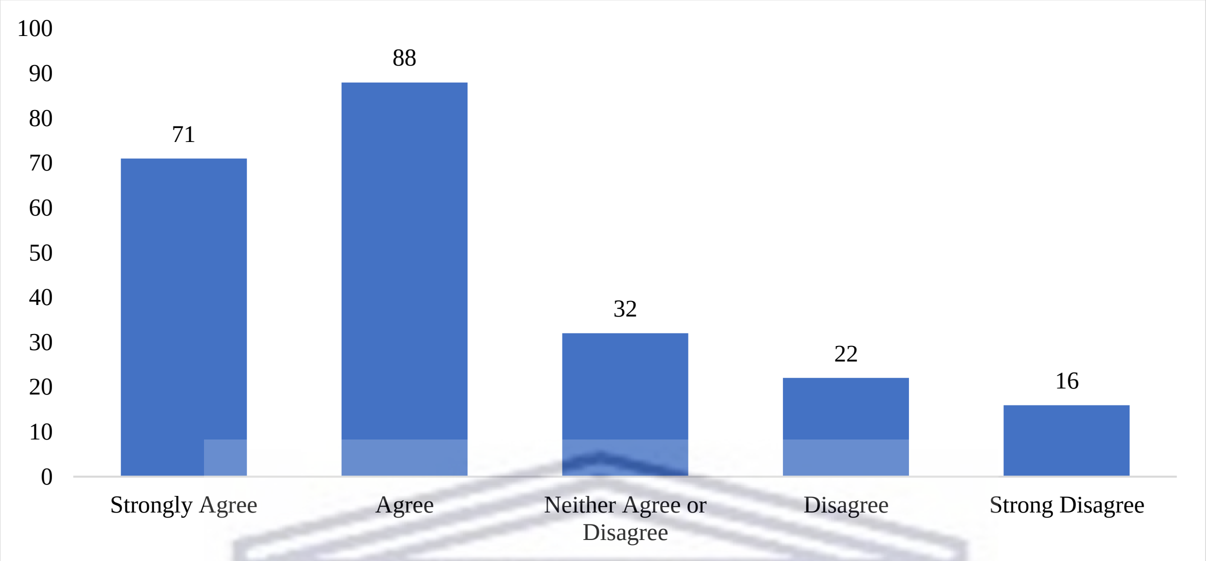


Figure 6.16 Accessibility of guidelines

I know where to access the cybersecurity guidelines for the institution.				
		Frequency	Per cent	Valid Per cent
Valid	Agree	88	38.4	38.4
	Strong Agree	71	31.0	31.0
	Neither Agree nor Disagree	32	14.0	14.0
	Disagree	22	9.6	9.6
	Strong Disagree	16	7.0	7.0
	Total	229	100.0	100.0
Median		Agree		
Mode		Agree		

Table 6.15 Accessibility of guidelines

6.4.12 The Training Offered by The Institution Helps Me to Understand Cybersecurity And How To Protect Myself And The Institution

SETAs are identified in the literature as critical pillars supporting cybersecurity in institutions. This is because often, due to their lack of knowledge, employees end up being the greatest threat to corporate information security (Mitnick *et al.*, 2002). Hwang *et al.* (2019) stated that security awareness occurs when employees are exposed to SETA. Through SETA, compliance with the security policies set out by organisations is more likely to occur. The responses to the statement posed to respondents showed that 46.7 per cent of the respondents "Strongly agreed" with the statement about the effectiveness of the training offered by the institution. 35.4 per cent "Agreed" with the statement, only a few respondents were neutral about the training offered, and an even smaller percentage said that the training provided did not help them in any way. Figure 6.17 shows the responses.

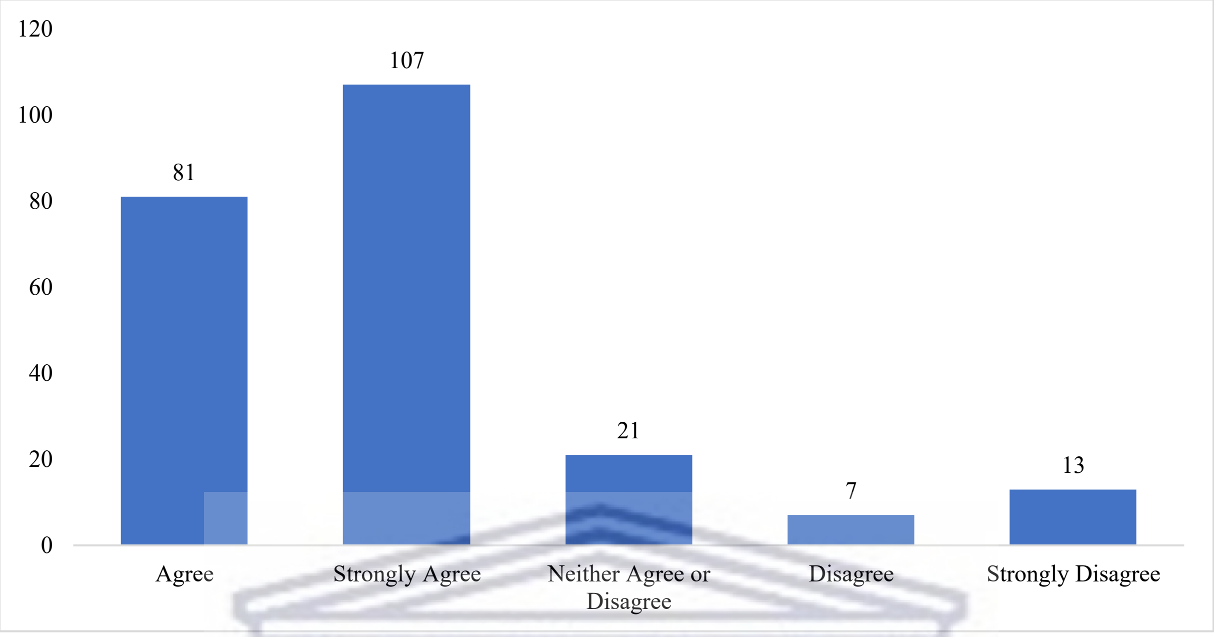


Figure 6.17 Security Education, Training and Awareness

The training offered by the institution helps me understand cybersecurity and how to protect myself and the institution.				
		Frequency	Per cent	Valid Per cent
Valid	Agree	81	35.4	35.4
	Strongly Agree	107	46.7	46.7
	Neither Agree nor Disagree	21	9.2	9.2
	Disagree	7	3.1	3.1
	Strongly Disagree	13	5.7	5.7
	Total	229	100.0	100.0
Median		Agree		
Mode		Strongly Agree		

Table 6.16 Security Education, Training and Awareness

6.4.13 I am aware of the cybersecurity frameworks the institution has adopted.

In line with the theme of awareness within institutions, this statement sought to investigate the respondents' familiarity with the security framework within the institution that employed them. Knowledge of the framework potentially makes it easier for employees to adhere to guidelines as they know the driving force of the policy. The responses indicated that 40.2 per cent were aware of the framework. 40.2 per cent of the respondents indicated that they "Strongly Agreed" with the statement and 30.1 per cent "Agreed" with the statement. Those who disagreed with the statement cumulatively comprised 13.6 per cent of the respondents. Figure 6.18 below shows the responses.

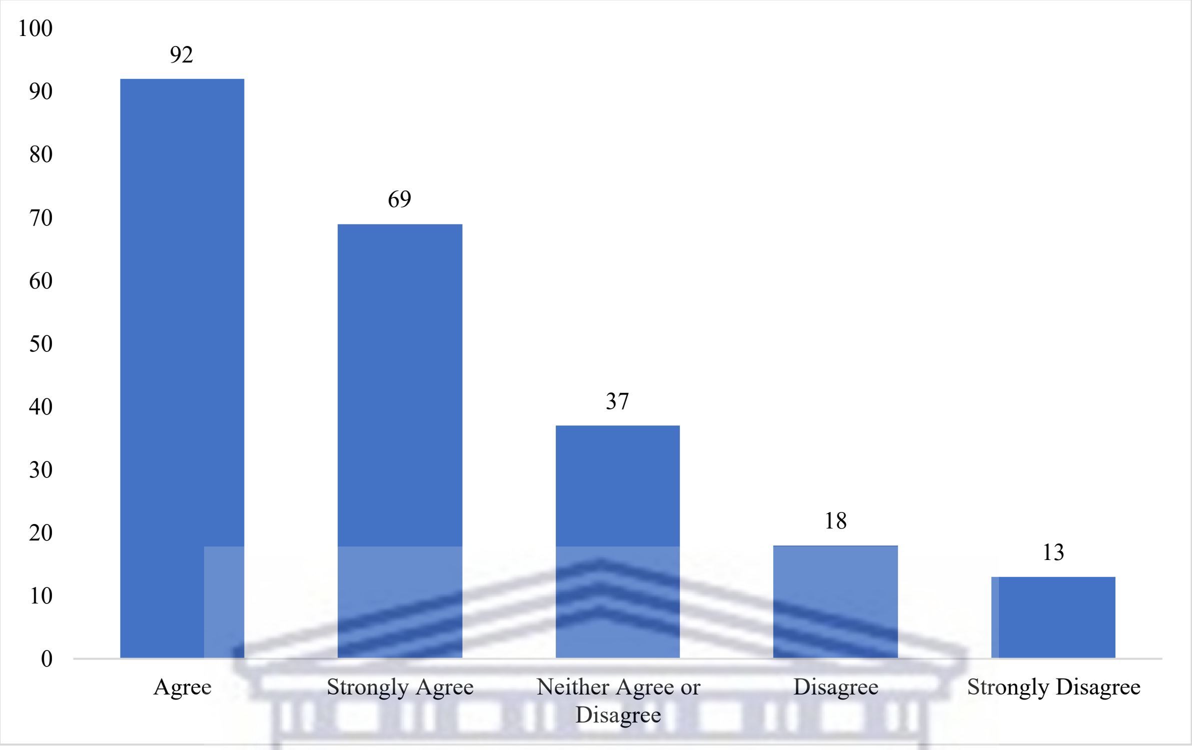


Figure 6.18 Knowledge of the adopted framework

I am aware of the cybersecurity frameworks the institution has adopted.				
		Frequency	Per cent	Valid Per cent
Valid	Agree	92	40.2	40.2
	Strongly Agree	69	30.1	30.1
	Neither Agree nor Disagree	37	16.2	16.2
	Disagree	18	7.9	7.9
	Strongly Disagree	13	5.7	5.7
	Total	229	100.0	100.0
Median		Agree		
Mode		Agree		

Table 6.17 Knowledge of the adopted framework

6.4.14 I am aware of the impact cyber-attacks have on the institution.

The above statement was posed to respondents to investigate if they were aware of the impact cyber-attacks (cybercrimes) have on financial institutions. The assumption behind the statement was that if respondents were aware of the attacks at other financial institutions, they were less likely to engage in behaviour that would undermine their organisation's security. De Kimpe, Walrave, Verdegem and Ponnet (2021) found that when users perceived themselves as more knowledgeable on cybersecurity issues, they thought of themselves as less vulnerable to cybercrimes and, as such, were less likely to take further steps to protect themselves. More than half of the respondents indicated that they were aware of the impact of cyber-attacks on commercial banks. As shown in Figure 6.1 below, 86.1 per cent of the respondents either Agreed or Strongly Agreed with the statement, and only 5.7 per cent disagreed with the statement, as shown in Figure 6.19.

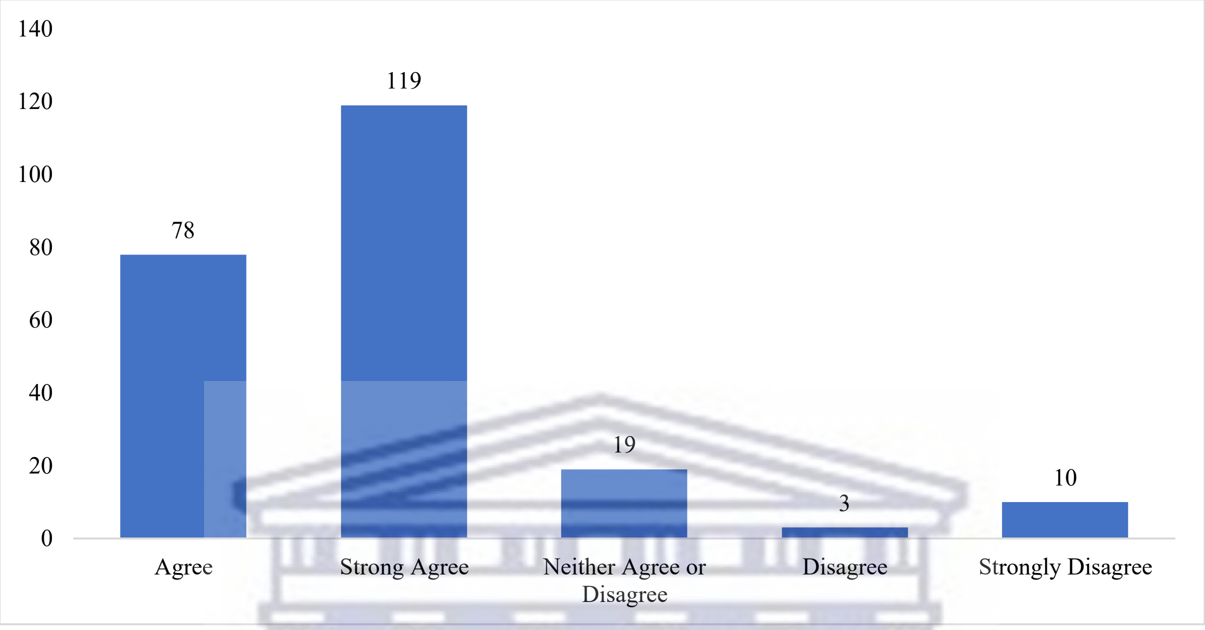


Figure 6.19 Impact of cyber-attacks.

I am aware of the impact cyber-attacks have on the institution.				
		Frequency	Per cent	Valid Per cent
Valid	Agree	78	34.1	34.1
	Strong Agree	119	52.0	52.0
	Neither Agree nor Disagree	19	8.3	8.3
	Disagree	3	1.3	1.3
	Strongly Disagree	10	4.4	4.4
	Total	229	100.0	100.0
Median		Strongly Agree		
Mode		Strongly Agree		

Table 6.18 Impact of cyber-attacks.

6.4.15 I am aware of some of the cyber threats faced by commercial banks in South Africa.

Much like the rest of the world, South Africa is not immune to cyber-attacks, and financial institutions in the country have faced their fair share of attacks in recent history. The above statement sought to investigate whether respondents employed in banks were aware of the threats South African banks have faced in recent history. This statement sought to understand if awareness of cyber threats impacted how respondents behaved within their institutions. Given the numerous cyber-attacks that have taken place recently, a phenomenon defined as cyber stress has emerged. Kaspersky Lab (2018) stated that people are becoming progressively worried about cybersecurity threats and attacks, with 81 per cent of their respondents stating that news of cyber incidents caused them personal stress. Most respondents indicated they were acutely aware of local banks' cyber threats. Almost half of the respondents (83.4 per cent) indicated they were aware of the threats. Only 9.6 per cent of the respondents neither agreed nor disagreed with the statement, and 6.9 per cent stated they were unaware of the threats. The responses are shown in Figure 6.20

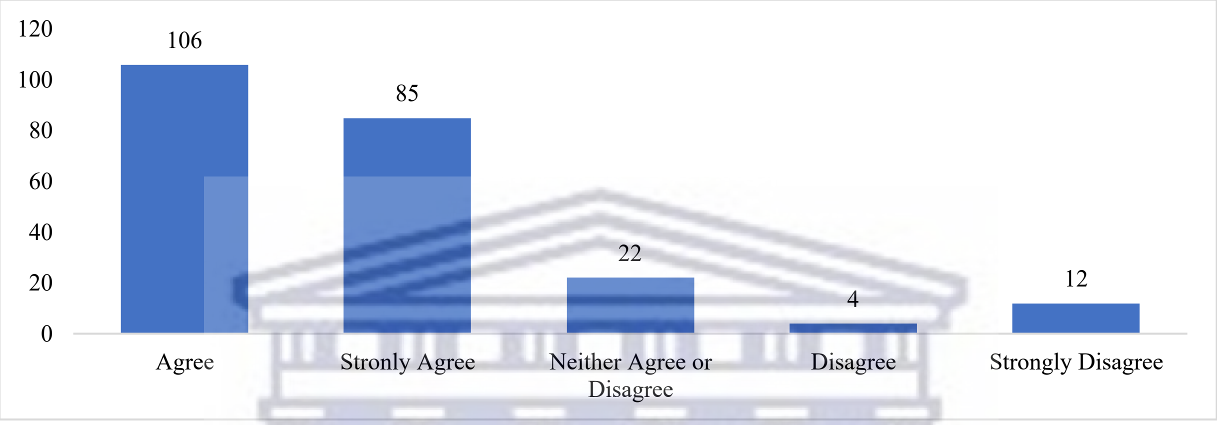


Figure 6.20 Threats faced by South African banks.

I am aware of some cyber threats commercial banks face in South Africa.				
		Frequency	Per cent	Valid Per cent
Valid	Agree	106	46.3	46.3
	Strongly Agree	85	37.1	37.1
	Neither Agree nor Disagree	22	9.6	9.6
	Disagree	4	1.7	1.7
	Strongly Disagree	12	5.2	5.2
	Total	229	100.0	100.0
Median		Agree		
Mode		Agree		

Table 6.19 Threats faced by South African banks.

6.4.16 I am aware of cybersecurity incidents that have happened at other commercial banks.

Since cybercrimes are a global phenomenon, this statement sought to interrogate the respondent’s awareness of cyber incidents beyond the borders of South Africa. Guermazi (2021) posited that cybersecurity risks had become global and that taking a coordinated and collaborative approach to deal with the risks would benefit the world. The United Nations also recognised the global threat cybercrimes pose to nations and, in response to the matter, has created an international programme on cybercrime to assist member states with cyber-related crimes (United Nations, n.d.) Most respondents (68.5 per cent) agreed or Strongly Agreed with the statement. This shows that the respondents were acutely aware of the attacks commercial banks are suffering across the globe. 16.2 per cent of the respondents were neutral to the statement, while cumulatively, 15.2 per cent were unaware of the cyber incidents that happened at other commercial banks. Figure 6.21 shows the responses.

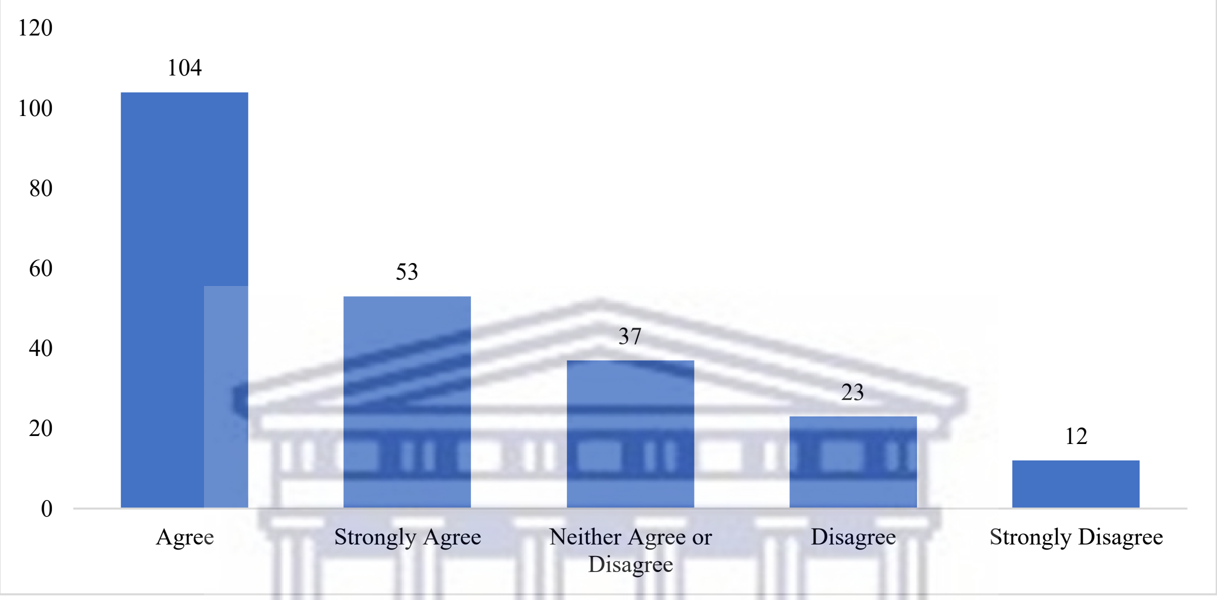


Figure 6.21 Cyber-attacks against other banks.

I am aware of cybersecurity incidents that have happened at other commercial banks.				
		Frequency	Per cent	Valid Per cent
Valid	Agree	104	45.4	45.4
	Strongly Agree	53	23.1	23.1
	Neither Agree nor Disagree	37	16.2	16.2
	Disagree	23	10.0	10.0
	Strongly Disagree	12	5.2	5.2
	Total	229	100.0	100.0
Median		Agree		
Mode		Agree		

Table 6.20 Cyber-attacks against other banks.

6.5 Confirmatory Factor Analysis

The following section applies CFA to the data collected in the study and confirms relationships between factors that could affect cybersecurity within a commercial bank. Mueller and Hancock (2001) showed that one of the benefits of CFA is its ability to provide investigators with helpful information about how well data fits a specific theory-derived measurement model.

6.5.1 CFA Process

CFA falls under the umbrella of structured equation modelling, which allows for examining causal relationships among latent and observed variables in a model derived from theory. Tavakol and Wetzel (2020) stated that CFA is a theory-driven approach that assesses how well data fits a proposed model or theory. Before analysing the data, researchers must first identify a factor model. Specifically, CFA investigates the internal relationships between variables. Suhr (2005) outlined eight steps in the CFA process: **i)** *review of relevant theory and research literature to support model specification,* **ii)** *specifying model,* **iii)** *determining model identification,* **iv)** *collecting data,* **v)** *conducting preliminary descriptive statistical analysis,* **vi)** *estimating parameters in the model,* **vii)** *assessing model fit, and* **viii)** *presenting and interpreting the results*.

These steps involved formulating a hypothesis based on theoretical knowledge, empirical research, or both. The researcher then postulated that the relationship pattern statistically tests the hypothesis (Suhr, 2005). The choice of CFA in this study was informed by the researcher's initial assumptions that there were relationships between identified factors based on the collected literature and survey data.

6.5.2 Hypothesis

CFA may be used to test the hypothesis that a relationship exists between the observed variables (those variables made up of data measured by the researcher) and the latent variables of those observed variables. Latent variables cannot be observed but can be detected by their effects on observable variables. An initial hypothesis was established through the literature and the data collected during the study. The initial hypothesis postulated that there was a relationship between the five observed variables, which were security posture (SP), security awareness (SA), threat awareness (TA), security training (ST) and human behaviour (HB). The null hypothesis averred that no relationship existed between the variables. This hypothesis was based on information in the literature review, which identified multiple factors that influence cybersecurity within organisations.

6.5.3 Initial Model

The initial model serves as a formal depiction that reflects the a priori assumptions about the measurement model (Sarmento & Costa, 2019). To construct the model, sixteen observable variables were used. These variables were Likert items that made up the survey distributed to respondents. From the sixteen observed variables, five latent factors were identified. The five factors were security posture (SP), security awareness (SA), threat awareness (TA), security training (ST) and human behaviour (HB). SP was a latent factor with six observed variables from the survey; SA was made up of two observed variables; TA had three observed variables; ST also had three variables, while HB had two observed variables. Figure 6.22 depicts the model used to assess the covariance of the latent variables.

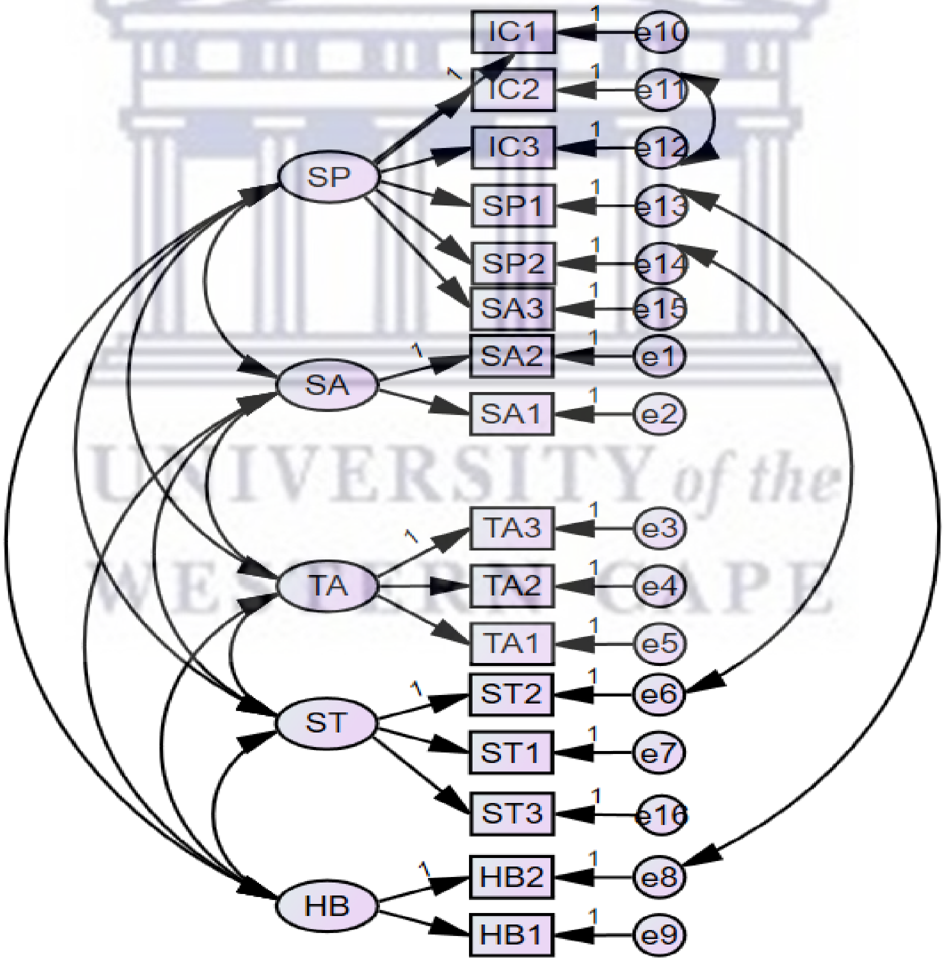


Figure 6.22 Initial Model

6.5.4 Model Results

Several indicators of fit and their criteria were used to assess the model's results to examine how well the data fit the model. Goodness-of-fit index (GFI), Adjusted goodness-of-fit index (AGFI), Normal fit index (NFI), Tucker-Lewis Index (TLI), comparative fit index (CFI) and root mean square error of approximation (RMSEA) were used as indicators. The covariance of the latent variables was used as a measure to assess the relationship between the variables. Figure 6.23 depicts the results of the model. The model results show that relationships exist between all latent variables, although the relationships vary in significance. The correlation matrix in Table 6.22 shows this.

Table 6.21 Covariance matrix

Variable	*SP*	*HB*	*ST*	*TA*	*SA*
SP[13]	.581				
HB[14]	.519	.670			
ST[15]	.609	.527	.732		
TA[16]	.547	.576	.662	.711	
SA[17]	.609	.598	.813	.649	.842

Table 6.22 lists the results of the model fit indices, and Figure 6.23 depicts the computational results of the model. CMIN is the chi-square value traditionally used as an index for assessing a model for goodness-of-fit. Kline stated that in this case, the chi-square value is used to test for the exact-fit hypothesis, which in turn states that there is no difference between the covariances predicted by the model, the parameter estimates and the population covariance matrix (Kline, 2016); while DF refers to the degrees of freedom, and P is the significance level. GFI and AGFI values typically range from 0 to 1, with values closer to 1 indicative of an acceptable model. The value of GFI is .911, which indicates an acceptable model, while AGFI is slightly less than .90 with a value of .867 (Pituch & Stevens, 2016). NFI, RFI, IFI, and TLI are incremental and comparative fit indices. Crowson (2020) posited that values greater or equal to .90 indicate an acceptable fitting model. The indices to indicate an acceptable model fit are RMSEA, LO 90 and HI 90, which are confidence intervals and PCLOSE. Kline (2016)

[13] Security Posture
[14] Human Behaviour
[15] Security Training
[16] Threat Awareness
[17] Security Awareness

stated that RMSEA values below .05 indicate close-fitting models. However, values between. 05 and. 08 indicate an adequate fit if the upper bound (HI 90) is less than. 10, and the lower bound (LO 90) is more significant than. 05, which is the case with our model, which suggests that our model has an acceptable fit (Pituch & Stevens, 2016).

Table 6.22 Model Fit

Measure	***Value***
CMIN	187.284
DF	91
P	.000
GFI	.911
AGFI	.867
NFI	.917
RFI	.891
IFI	.956
TLI	.941
RMSEA	.068
LO 90	.054
HI 90	.082
PCLOSE	.018

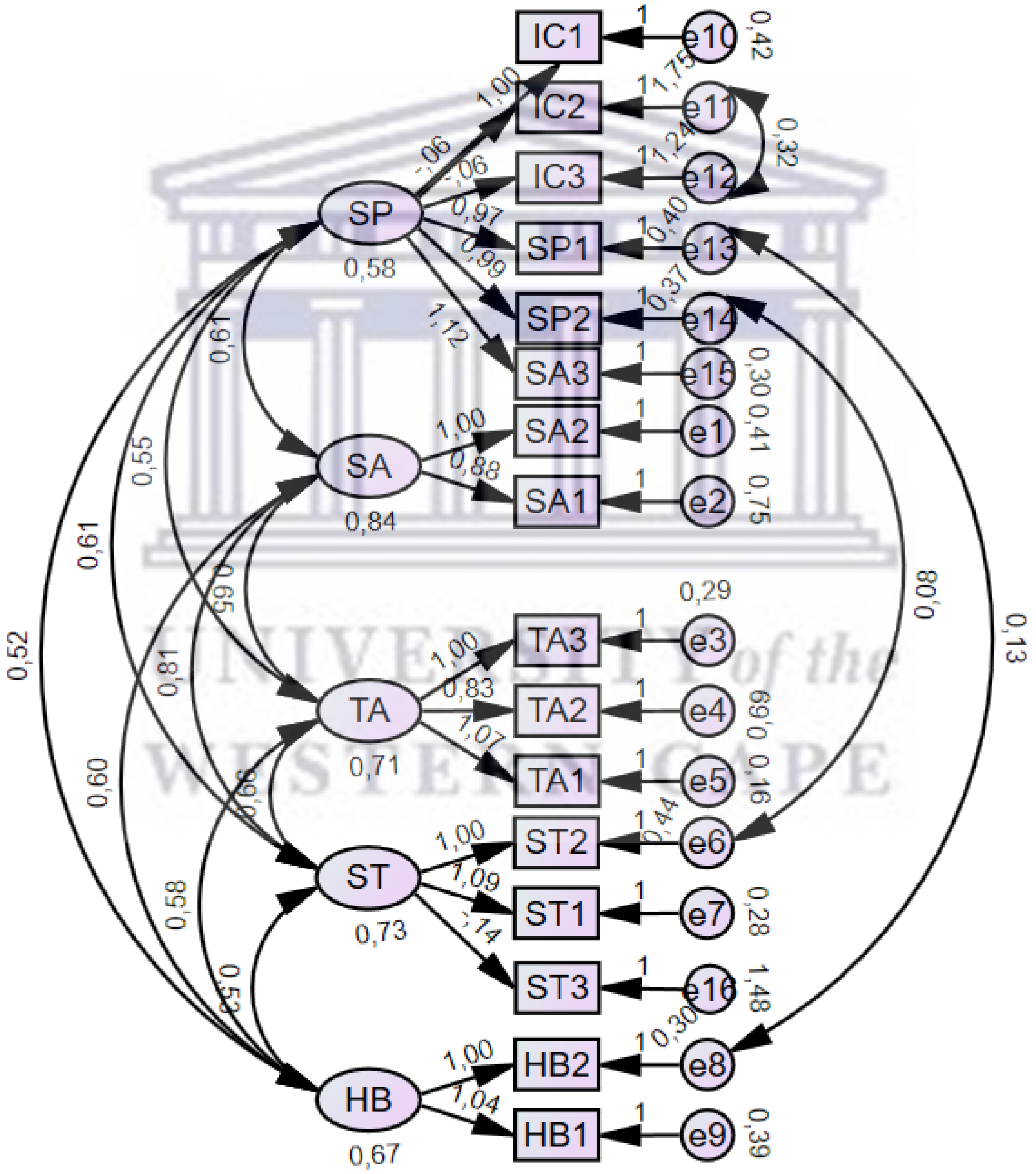


Figure 6.23 Model results

6.6 Chapter Summary

This chapter briefly restated the data collection process for the study's quantitative data aspect. Then, a succinct description of the profile of the respondents was given, and the demographic details of the respondents were presented and discussed, followed by a descriptive statistics component that sought to examine the distribution of the responses for each of the sixteen Likert item questions that were posed to the respondents. Structural equation modelling followed after the descriptive statistics in the form of a CFA analysis, which investigated the hypothesis that a relationship exists between the latent variables of the survey. A discussion of the computational results of the CFA was given alongside the hypothesised model.

PART V

Chapter Seven : Conclusions, Recommendations, And Future Research

7.1 Introduction

The last chapter summarises the study by briefly discussing the six previous chapters. The first part of the chapter focuses on brief conclusions drawn from the six previous chapters. Secondly, the chapter considers the findings from the study's qualitative and quantitative chapters. It then synthesises the research into conclusions based on the qualitative and quantitative findings while considering the literature. Then, the chapter makes recommendations that may be applied in practice to support the cybersecurity initiatives of a financial institution within its cybersecurity framework. Some limitations of the study are stated, and suggestions are made for future studies that could continue the work presented in the study.

7.2 Triangulation Of Qualitative And Quantitative Findings

Denzin (2015) defined triangulation as applying and combining several research methods to study the same phenomena. Carugi (2014) further stated that synthesis and triangulation of multiple data sources strengthen the quality and creditability of a study and the recommendations thereof.

7.2.1 Demographic Characteristics

The following subsection discusses the similarities and differences between the demographic characteristics of the respondents and participants of the study. Table 7.1 below shows the similarities and differences.

Table 7.1 Demographic data triangulation

Demographic variables	Quantitative findings	Qualitative findings	Discussion
Gender	Ninety-two females One hundred thirty-five males, Two respondents who chose not to reveal their gender completed the survey.	Seven females Fourteen males	In qualitative data collection, females comprised 33.33 per cent of the participants. In the quantitative data, females constituted 40.17 per cent of the respondents. Although gender proportions

			were unequal, their difference was not a significant factor.
Age	18-25: 43 26-35: 169 36-45: 10 46-55: 6 Older than 56 years: 1	Thirteen participants were aged between 26 and 45 years old. Two (2) participants were aged between 18 and 25. Six (6) participants were aged between 36 and 46 years. Zero (0) participants were older than 47	The age distribution for respondents and participants showed the most significant number of participants' ages ranged between 25 and 46 years old. However, the quantitative data showed that some respondents were over 46.
Highest qualification	Matric: 3 Certificates: 4 National Diploma: 29 Bachelor's Degrees: 79 Honour's Degrees: 81 Master's Degrees: 30 Doctorate Degrees: 3	Eleven participants held bachelor's degrees. Five participants held master's degrees. Four participants held honours degrees.	The quantitative and qualitative data collection showed that most respondents had higher qualifications. However, in the quantitative data, an insignificant number of respondents had either no certificates or matric certificates.
Years of working experience	Less than one year: 9 1-5 years: 100 6-10 years: 64 11-20 years: 48 More than 21 years: 8	Nine participants had between 1- and five years of working experience. Six participants had working experience between 6 and 10 years. Five participants had work experience between 11 and 20 years. One participant had more than 20 years of work experience.	The qualitative data converged with the quantitative data concerning most respondents and participants having work experience ranging between 1 and 5 years. Furthermore, fewer respondents with working experience, more significant than 21 years, were observed.

7.2.2 Similar Qualitative and Quantitative Findings

The study employed a mixed methods research design. The researcher had to collect qualitative and quantitative data by adopting that research approach. This subsection discusses the similarities between the data collected in the respective data collection methods. It also discusses the differences that were identified in the data.

The Influence of Human behaviour

One of the key themes that emerged from the qualitative findings was the influence HB had on an organisation's SP. This was noted by participants who highlighted the users with limited technical proficiency from an internal(employees) and external(customers) perspective, who usually posed the highest risk to an organisation's security. From qualitative findings, the influence of HB was observed under the themes of i) *insider threats, ii) poor cybersecurity culture, iii) users with limited technical proficiency, and iv) humans being key to a practical framework.* From the quantitative data, the influence of HB was measured by consulting a section in the survey, which comprised three questions about the role of HB. From the questions posed, the overwhelming majority of participants indicated that they were aware of how their actions and those of other users and customers impacted the SP of the commercial banks.

Security posture

Various actions need to be taken to bolster an organisation's posture. The data showed that the respondents and participants indicated that although the banks were making decent strides in improving their posture, there was still room for improvement. The participants stated that there was room for improvement in the security framework. They commented on how their organisations' security hygiene and culture improvements are needed. The respondents also highlighted how some of the rules hampered their ability to carry out their tasks and how, given the right circumstances, they were prepared to circumvent the restrictions imposed by the banks. Such action would lead to a weakening of the overall posture in organisations.

Security training and awareness

The data from the study’s qualitative and quantitative aspects showed the importance and effectiveness of ST in organisations. In both data sets, it was established that ST was an effective intervention for improving an organisation's security. The respondents indicated how the training offered by the respective banks enabled them to follow policies and procedures set up by the banks. Some participants emphasised how the training reduced the likelihood of staff members or management becoming victims of phishing and other social engineering attacks. SA was highlighted as one of the vital contributors to the security of commercial banks by both data sets (qualitative and quantitative data). The semi-structured interviews, which informed the qualitative data, showed that participants expressed how an awareness of their corporate security responsibilities aided in upholding a sound SP. They also highlighted how the knowledge of the cybersecurity framework enabled them to perform their duties with a clear understanding of the security restrictions imposed on them. Similar findings were found in the quantitative data. From the data, it was evident that most respondents were aware of security, as evidenced by respondents indicating that they were aware of the frameworks within their respective commercial banks and of the threats commercial banks face in cyberspace.

Threat awareness

Both the qualitative and quantitative data showed that the respondents and participants indicated that they were aware of the threats commercial banks face. Most respondents highlighted this by stating that they were aware of the attacks at other commercial banks in the country and of the impact of cyber-attacks on banks' operations. The themes that emerged from the qualitative data indicated that cyber-attacks' impact on banks was also noticed. Participants indicated that successful attacks had the potential to disrupt and bring the normal operations of a bank to a halt.

7.3 Conclusions

7.3.1 Conclusions Drawn from the Literature Review

The study sought to address the four research objectives by reviewing the literature. This subsection summarises the findings from the literature concerning the research objectives and the study's research questions.

From the media reports and articles, it was evident that the success of attacks was dependent on multiple factors. The factors identified from media reports and articles showed that malicious employees (insider threats) and users with limited technical proficiency (end-users) would often use social engineering attacks as an initial vector to gain access to user accounts. Then, they would be able to carry out their malicious attacks. In some rare cases, the success of the attacks was attributed to advanced attackers who took advantage of weak controls within banks. A concerning trend observed in the literature was the increase in attacks carried out by employees within the banks. Furthermore, a lack of skilled cybersecurity personnel was highlighted as one of the issues leading to successful cyber-attacks. This may be attributed to the lack of security personnel, which means that banks cannot adequately identify the perpetrators to respond to cyber threats. This phenomenon, however, was not unique to South Africa. Globally, there is a shortage of cybersecurity professionals.

Regarding the exact interventions adopted by commercial banks in South Africa, there needs to be more data from the literature to identify the exact interventions banks in South Africa are taking to protect themselves. What was evident, however, was the advancements the government of South Africa was making in enabling the persecution of cybercrimes using the Cybercrimes Act and advancements in protecting personally identifiable information belonging to citizens of the republic. The South African Reserve Bank, a prudential authority, and the FSCA did, however, mandate banks and other financial institutions in South Africa to comply with a joint standard on cybersecurity and cyber resilience, which set out requirements for sound practices and processes around cybersecurity and cyber resilience. In conjunction with these requirements, banks had to comply with PCI-DSS when they processed credit card details. All these requirements and advancements in legislation could be considered part of the interventions banks have adopted to address cyber threats and attacks.

The information in the literature adequately captured the impacts of cyber-attacks and cybercrimes. The effect of cyber-attacks on commercial banks was mostly monetary, with one of the most memorable financial losses being ZAR 300 million, which Standard Bank South Africa suffered. However, given that some of the commercial banks in South Africa are publicly traded companies, the impact of the cyber-attacks they experienced was far more than just the monetary losses from the attacks. In certain instances, their share price was negatively affected, as well as public perception, although these effects were often not long-term. Reports published by independent bodies and the banks themselves also showed that the frequency and variation of attacks experienced by commercial banks have increased recently. SABRIC stated that the number of cybercrimes reported in South Africa had sharply increased over the past few decades, and findings by van Niekerk (2017) supported the views expressed by SABRIC. It is evident that cyber-attacks have increased and that the sophistication of the attacks faced by banks has advanced recently.

7.3.2 Quantitative Conclusions

The quantitative section of the study analysed data gathered from a Likert scale survey distributed to respondents. The survey interrogated the respondents about their perception of cybersecurity within their respective banks, in line with the study's research objectives. They also sought to determine if there was a relationship between the themes being probed by the survey and how strong the correlations were. Five latent variables were identified from the data collected, each of which sought to address an aspect of cybersecurity within the banks. The latent variables that emerged were:

- Security Posture
- Human Behaviour
- Security Training
- Threat Awareness
- Security Awareness

The findings from the survey showed that there was a strong correlation between ST and the impact it had on HB within the organisation. A strong correlation between ST and SA was also observed, as well as between the SP of an institution and the ST offered to its employees.

7.3.3 Qualitative Conclusions

Qualitative data for the study was gathered using semi-structured interviews with participants from commercial banks in South Africa employed within the banks' IT, Risk or Compliance functions. The questions asked during the interviews were intended to address the three research objectives and some of the research questions for the study. The findings are summarised below. From the participant's responses, it was evident that there were multiple contributors to the success of attacks by threat actors. The factors are listed below:

- **Poor cybersecurity culture:**

Security prioritisations help organisations identify the potential risks threatening them and subsequently prioritise the defence of their digital assets (Blum, 2020). Although some participants occupied positions of influence, security was still not emphasised in their role, implying that their subordinates also did not see the importance of cyber safety. Keman and Pearlson (2019) stated that organisations' lack of a strong cybersecurity culture can make them less resilient against cyber-attacks. An organisation's robust cybersecurity culture greatly influences employees' inclination to adhere to cybersecurity controls.

- **Inadequate resourcing (human resources and financial resources):**

Kshetri (2019) highlighted the lack of cybersecurity skills and estimated that by 2020, there would be a shortfall of about 100000 cybersecurity personnel in Africa. The World Economic Forum (2022) and (ISC)^2 (2021) stated that there is still a workforce gap of more than 2.72 million positions globally, and the cybersecurity workforce needs to grow by 65 per cent to defend the critical assets of organisations effectively. The lack of resources included insufficient funding regarding the size of the budget apportioned to security, and the other resources included inadequate staffing of cybersecurity personnel. The European Union Agency for Cybersecurity (2021) supported the participants' views by positing that a lack of information, SA and expertise in organisations often leads to a lack of cybersecurity budget and inadequate staffing. Da Veiga *et al.* (2020) stated that resources are required for successful implementations or changes to information security within organisations; budgeting and funding are crucial to implementing security practices.

- **Users with limited technical proficiency:**

Van Niekerk (2017) stated that one of the first successful cybercrime incidents against a commercial bank was a threat actor who compromised a user's account by sending malicious mail to the user. This was not the last occurrence where threat actors viewed end-users as viable threat vectors. Over the years, countless other attacks have used unaware and negligent users to enter organisations' cyberspace. Mitnick *et al.* (2002) stated that employees and end-users were the greatest threat to corporate information security, intentionally or through negligence, or often due to lack of knowledge.

- **Misalignment between business objectives and security**

The misalignment of business needs and cybersecurity often leads to a misunderstanding of cybersecurity's role in organisations and its impact on helping organisations deliver their products and offerings. Edwards (2020) stated that a disconnect existed between how businesses understand and manage cyber risk, driven by organisations failing to view cybersecurity as a business strategy rather than merely an IT problem. Due to this limited scope of cybersecurity, an organisation's ability to analyse cyber risks and prioritise and execute remediation based on business criticality and threat context is hampered. When addressing the interventions employed by commercial banks, four themes emerged from the analysis of the responses given by the participants. It was evident that participants were acutely aware of some of the mitigation strategies adopted by the banks to combat cyber threats and crimes. The approaches undertaken by the banks are listed below:

- **Security controls**

Chapple *et al.* (2021) postulated that cyber controls fall into three categories: physical controls, technical controls, and administrative controls. IBM Cloud Education (2019) described security controls as ‘parameters implemented to protect various forms of data and infrastructure important to an organisation. Any safeguard or countermeasure used to avoid, detect, counteract, or minimise security risks to physical property, information, computer systems, or other assets is considered a security control.’

- **Security tools and assessments**

Various tools from multiple vendors are integral to gaining visibility into the modus operandi of an organisation and mitigating threats. Security and risk assessments are also tools in organisations' arsenal for gauging their SP and risk appetite. They serve as a guide for gathering recommendations on improving the security of applications and assets. Blum (2020) posited that risk management can be a keystone within an organisation’s security culture and governance model. Wang *et al.* (2021) also supported the participant's views by stating that risk assessments are essential to effectively responding to cyber-attacks. Their paper demonstrated how risk assessments assist in quantifying and identifying cybersecurity risks and finding attack paths with high cybersecurity threats.

- **Security training and awareness**

ST and awareness programmes can be vital for maintaining an organisation’s SP and building a robust security culture. SANS (2021) stated that there has been a shift in ST, moving from a compliance-focused initiative to playing a crucial part in an organisation’s ability to manage its human cyber risk. Awareness programmes further assist in disseminating an organisation’s security policy to its employees in the hope that these programmes will encourage a security-aware culture so that good security practices will become the de facto approach to everything in organisations (Gundu *et al.*, 2019). Regarding the impact of cyber-attacks on commercial banks, four themes emerged from the analysis of the responses. The responses showed that bank employees were aware of the consequences of successful cyber-attacks and the far-reaching impact of the attacks. The themes were:

- **Hampering operations**

One of the core tenets of cybersecurity is the CIA triad, which is concerned with confidentiality, integrity, and the availability of resources. An attack on either of those three pillars adversely affects a bank’s ability to render services securely and timeously to its clients (Chapple *et al.*, 2021). Material cyber-attacks can bring operations to a standstill. Banco Pichincha, Ecuador’s largest private bank, suffered that fate when a cyber-attack shut down portions of its network, which led to widespread disruption of services (Abrams, 2021)

- **Reputational damage**

Reputational damage and trade name devaluation are real consequences of cyber-attacks. Trust between the bank, its clients, stakeholders, and investors is usually eroded when they fall victim to cyber incidents. Agrafiotis *et al.* (2018) identified reputational harm as a harmful result of cyber-attacks. They stated that reputational harm adversely affects how the public perceives the organisation, and this might, in turn, affect how the media portrays the organisation and the relationship between the organisation and its stakeholders.

- **Financial losses**

Accenture (2019) posited that the annual cost of all cyber-attack types was increasing. The sentiment of participants was in line with global reports on cybercrimes. Within South Africa, the fines are imposed by the South African Reserve Bank and the Information Regulator, depending on the type of infringement. Examples of these fines include a ZAR 1 million to Habib Overseas Bank Limited for inadequate internal controls for detecting suspicious and unusual transactions; Investec Bank Limited was fined R20 million for a similar transgression, as well as Habib Overseas Bank (South African Reserve Bank, 2020).

Financial losses due to cyber-attacks were not only from regulatory fines; they could also emanate from the attackers successfully exfiltrating money from the bank, either through ransom demands for encrypted systems or breaches (Buckley, 2021).

- **Loss of investor and customer confidence**

The participants' views aligned with the literature findings that the announcements of successful breaches by hackers against organisations often negatively impacted the market value of the organisation’s stock price (Smith *et al.*, 2019). Loss of investor confidence was not the only ramification an institution would suffer from due to a cyber-attack. Participants also expressed how the customers of commercial banks could lose trust in the bank due to a cyber-attack. EY Global (2019) echoed the participants' views by stating that a cyber-attack could destroy trust between organisations and their customers. This is because, in recent times, customers have been providing more data to organisations.

7.4 Recommendations

The study uncovered several factors contributing to successful cyber-attacks on commercial banks in South Africa. The study also identified trends in the types of attacks experienced by the banks. This section draws on those findings to make recommendations to address the identified factors and trends.

For banks in South Africa to address the factors that lead to successful cyber-attacks, an approach that emphasises people, processes and technology needs to be adopted. This is because cybersecurity has become more than merely an issue that technology can solve, which only affects IT within organisations. It has become a unique mix of technologies, people, and processes, with processes often forming regulations, laws, and guidelines within organisations (Parent & Cusack, 2016). This study recommends that commercial banks in South Africa start making significant strides in investing in upskilling their existing employees to become security professionals. Price Waterhouse Coopers (2022) has characterised the current security talent shortage as a crisis.

As such, organisations cannot afford to wait for new talent to come into the workforce while they continue to digitise their offerings and expand their digital footprint. In addition to training and upskilling, the researcher recommends that the banks adopt better ways of driving awareness and training within their organisations. The banks must deliver awareness and training programmes that will leave a long-lasting impression on employees. Awareness must also be heightened among end-users(customers) who are often victims of cybercrimes, internal users, and professionals who might find themselves within the bank's risk, IT, compliance, or security domains.

Given the complexity and ever-increasing threat of cybercrimes, banks, as part of the nation's critical infrastructure and as key pillars to the functioning of the country's financial sector, should play a more active role in developing cyber legislation and cyber initiatives at a national level. The findings showed that the pace at which the government moves regarding cybersecurity and digital skills is far slower than what the industry is capable of. Through SABRIC, banks should lead the charge in suggesting actionable and practical legislation by sharing knowledge and information about the latest trends and threats. Banks could develop custom cybersecurity frameworks with the government and regional authorities for the South African context.

The findings also highlighted a lack of awareness and understanding regarding cybersecurity frameworks within banks. Participants in the study were often unclear about the frameworks the banks had adopted and what they entailed. Therefore, banks should make the security frameworks and policies governing decisions more accessible to professionals. This would better equip security professionals and facilitate open discussions about the direction and strategy that cybersecurity should follow. Furthermore, it should discourage the silos between departments responsible for frameworks and the people who are implementing the objectives of the frameworks (Lee, 2019). By adopting this approach, banks would embrace a shared responsibility philosophy for security and work towards embedding cybersecurity into the fabric of organisations (Sanders, 2016)

Cyber-attacks are inevitable for high-value institutions such as banks because they hold significant potential monetary gains for attackers and store substantial amounts of sensitive data, which is just as valuable for attackers. This could be attributed to data being seen as the new gold for organisations. Given that cyber-attacks cannot be avoided, The researcher recommends that financial institutions put in place processes and guidelines to respond to cyber incidents to limit the impact of the attacks. These processes should include:

- A cyber incident response plan.
- Creating a disaster recovery plan encompassing business continuity, data protection, data restoration and system recovery.
- Implementing risk transference and risk avoidance.
- Improve detection and response capabilities.

In addition, greater attention should also be given to the rise in insider threats. The number of attacks that have occurred with the assistance of employees or carried out by employees has increased, and as such, the banks should put more detections and deterrents to insider threats in place. This trend has also been fuelled by the ‘Great Resignation’ (Allen, 2022; Fischbein, 2022). An emphasis on cyber hygiene by banks would also serve to bolster security by eliminating the ‘low-hanging fruit’ and preserving the CIA of systems (Financial Sector Conduct Authority and the South African Reserve Bank, 2021)

Finally, the study recommends the adoption of the proposed conceptual cybersecurity framework. The framework aims to overcome the banking sector's cybersecurity challenges by proposing seven elements that banks could act on for an overall cybersecurity framework. The seven elements are cybersecurity resources, alignment of business and cybersecurity, practical and enforceable legislation, shared threat intelligence, cybersecurity awareness, cybersecurity culture, and understanding of cybersecurity. These elements would work in tandem to create a holistic approach to cybersecurity, improving organisations' postures.

7.5 Contributions Of The Study

7.5.1 Originality/Value

In recent decades, cybersecurity has moved from a problem seldom considered and often dealt with by IT professionals in basements typing away frantically on their keyboards, fending off hackers, to a business problem frequently discussed by executives in boardrooms. Cybersecurity has progressed from a technology risk to a business risk due to its threat to business operations (Gartner, 2021). Organisations and governments have become increasingly vulnerable to cyber threats because of how tightly integrated digital information and technology have become in day-to-day operations. Concerning research, originality may be defined broadly as producing new findings and theories or using a new approach, theory, method, or data (Guetzkow *et al.*, 2004).

Based on the above definition, for this study, the researcher sought to propose a conceptual Cybersecurity Framework for Commercial Banks in South Africa, which, after reviewing numerous studies, the researcher was convinced had never been attempted before. Given the critical nature of the banking sector in the country, the researcher was convinced that this study would add value to the cybersecurity and banking domains in South Africa.

7.5.2 Theoretical and Methodological Contributions

The development of a conceptual cybersecurity framework brought together multiple theories that aided in pointing out the factors that have led to successful cyber-attacks in recent times and identifying the trends in the type of attacks that commercial banks face. Seven factors that continually interacted with each other to produce complex and unpredictable relationships were identified. In light of the findings, the study proposed a theoretical CFA model to validate and further highlight the correlations between the identified factors. The study also takes a unique approach to generalising its findings by collecting data from various banks in South Africa, not just a single bank. Therefore, the study findings could be applied to the entire banking landscape in the country, not just one bank, thereby adding to the existing cybersecurity knowledge within the information systems domain.

7.5.3 Practical Contributions

The practical contributions of the study are recommendations that commercial banks may adopt to continue improving their existing approach to cyber defence and awareness. The recommendations are based on the literature and gaps identified from the data collection phase. Commercial banks need to treat cybersecurity with the urgency it needs due to the potential impact a successful attack might have on a bank's operations and the losses that might be incurred. The study identified multiple factors that contributed to the lack of cybersecurity frameworks within the commercial banking space in South Africa. It also uncovered recent factors that led to successful cyber incidents that could be addressed to continue improving the banks' SP.

This study also emphasises the need for South African banks to adopt a holistic approach that addresses people (employees and customers), processes (laws, regulations, and standards) and technology. To overcome the global phenomenon of skills shortage in security, the banks should take a proactive approach by upskilling and developing talent within their ranks instead of waiting for new talent to become available on the market. Greater emphasis must be placed on retaining existing talent and fostering employee knowledge sharing.

7.6 Limitations Of The Study

The study encountered methodological limitations, the first being data collection. With the implementation of POPIA, which limits the sharing of personal information without the express consent of the data subjects, the implications were that identified participants and respondents to the study could not share details of potential respondents and participants without first acquiring their consent. This limited the effectiveness of snowball sampling. Secondly, although the researcher tried to obtain permission from commercial banks to conduct the study within the banks themselves, consent was not given. Furthermore, most of the survey respondents and the participants of the semi-structured interviews were employees from the big five commercial banks in South Africa who account for about 89.4 per cent of all banking assets within the country (South African Reserve Bank Prudential Authority, 2020). Consequently, the study's findings mainly portray views concerning the big five banks.

Additionally, newer entrants into the banking space of the country were not presented in the study; these more recent entrants are taking a digital-only approach, as opposed to traditional banks, which had to modernise their services to meet the demands of customers who require more digital offerings. Regarding previous cyber incidents, the researcher could also not obtain detailed reports from the last security breaches experienced by commercial banks. The researcher had to rely on publicly available reports in media publications on previous cyber incidents in the country, which often did not give detailed information about the failure of controls that led to successful attacks.

7.7 Future Research

South African banks embraced digitisation and are leading the charge in providing the latest digital offerings to their customers by introducing innovative ways of interacting with banks and moving away from the traditional model of what a bank is. The country's banks are putting more of their offerings on the Internet for clients, and there has been a shift to platform banking in the country, with the banks adopting a model that would see them become a one-stop shop for their customers. Although customers welcome these advancements, which add value to the banking experience, they also increase the attack surface the banks expose themselves to. These advances in the digital space have not gone unnoticed by threat actors across the globe, and South Africa has become one of the primary targets in Africa for cybercriminals worldwide. The number of attacks that critical institutions in South Africa have experienced has steadily increased. The study showed that the cybersecurity field is something that commercial banks are still coming to grips with, and they are doing their utmost to address the challenges that arise. Thus, there are future-related research areas that academia could focus on concerning cybersecurity within the country. Some of those are listed below:

I. Although research measuring the impact of the new laws on cybersecurity within the country may be conducted, and given that these new regulations and rules were highlighted during the study, further research must be performed to investigate the impacts they have on commercial banks and to determine whether the regulations have had a positive effect on cybercrimes and cybersecurity within the country. The laws are the Cybercrimes Act and the POPIA.

II. To gather a more comprehensive picture of the threats and patterns of attacks faced by banks, further studies could focus on obtaining the necessary permissions and clearance to study these threats against the banks. Due to its sensitivity, this will enable better data collection and access to information that is not publicly available. In addition, an investigation into how the frameworks within banks are developed to support cybersecurity should also be carried out.

III. Information sharing was determined to be a vital tool in aiding organisations to stave off attackers and threat actors. This study did not focus on the intricate inner workings of how commercial banks and other key infrastructure providers interact with threat intelligence. Future research could focus on how SABRIC's role facilitates information sharing amongst commercial banks and other critical infrastructure services in the country. Furthermore, an analysis of how the different sector CSIRTs operate and share information should be conducted to foster a national ICAS.

IV. The conceptual model developed in the study could be validated by applying it to commercial banks. Furthermore, the insights from the study may be used to increase the model's validity and fine-tune it based on the feedback from participating banks. Research on the framework's effectiveness in addressing the challenges faced by commercial banks should also be conducted with banks and cybersecurity practitioners to provide further insights.

V. The study established that allocating resources to cybersecurity objectives in organisations is crucial for assisting organisations in protecting their assets from threat actors. As an area of future research, a study could analyse the allocation of resources to cybersecurity initiatives in commercial banks in South Africa and how the varied allocation of resources impacts banks' ability to defend themselves against threat actors. This could also be done in conjunction with studying an optimum approach to resource allocation.

7.8 Final Conclusion

The motivation behind this study was the researcher's exposure to cybersecurity in various commercial banks in South Africa. The researcher had the privilege of witnessing first-hand the copious work that goes into protecting commercial banks from threat actors and the unimaginable coordination in incident response processes. From then on, the researcher attempted to devise a solution to aid banks in dealing with cyber threats and attacks by developing a conceptual framework. This desire culminated in a research proposal in 2019, which, after approval, led the researcher on this fulfilling journey to understand better cybersecurity from technical, process, and human dimensions. The first chapter investigated how a cybersecurity framework could support commercial banks against threats and attacks. In that chapter, a detailed description of the background of the research and the challenges facing commercial banks concerning cybersecurity were discussed in-depth. The background section of the study covered issues such as the increase in cybercrimes witnessed within the country, the different types of cyber-attacks targeted at financial institutions in recent history, and the country's response to cybersecurity through the use of the national policy framework and POPIA.

The impact COVID-19 had on cybercrimes was also discussed, as it contributed to the number of cybercrimes committed in recent times. A brief overview of the mixed methods data approach used for the study was also discussed. The chapter also covered the objectives of the study, the problem statement, the study's purpose, and the study's originality and contribution to the academic body of knowledge around cybersecurity in South Africa.

The second chapter covered the literature review, an overview of published literature, information on cybersecurity, and the cybersecurity landscape in South Africa. It also discussed the difference in definitions of cybersecurity and information security. Literature on the key factors contributing to good SP was also discussed and contrasted with its detractors. The chapter also covered recent cyber-attacks on commercial banks in South Africa and attacks on the international stage that garnered copious attention from other financial institutions. The chapter concluded by identifying the gaps in the literature, which paved the way for some of the findings in the study.

The third chapter homed in on the theoretical frameworks that steer and underpin discussions around the NCPF that were used to guide the legislation and discussions around cybersecurity in the country from a national level. Other supporting frameworks, such as chaos theory, systems thinking, and complexity theory, were also covered. The chapter also discussed how all the mentioned theories could be applied to cybersecurity in a way that supports improving the posture of financial institutions, given the constraints identified in the literature. Gaps in the theoretical frameworks were also presented, and from those gaps, a conceptual model, which comprises seven elements, was proposed.

The fourth chapter covered the research design and methodology employed in the study for data collection and analysis. The study employed a mixed methods approach, which required collecting qualitative and quantitative data from each methodology that could be used to support the findings. The chapter also explored the different research paradigms and philosophies in the information systems domain and discussed the chosen paradigm. A discussion on the research strategy and the other data collection tools employed in the study also took place. These tools included semi-structured interviews for the qualitative aspect of the research, and a survey was distributed using Google Forms for the quantitative part of the study.

The fifth chapter presented and discussed the findings of the qualitative aspect of the study. The qualitative element included semi-structured interviews on video conferencing software (Zoom and Microsoft Teams). The interviews were transcribed, and an analysis was conducted on transcribed data. The questions posed to the study participants sought to address some of the research questions and objectives. Some findings aligned with what was identified in chapter two as detractors of good security postures for financial institutions, and others highlighted challenges that are believed to be endemic to South Africa.

The sixth chapter presented and discussed the study's quantitative findings. The quantitative data was collected over a year and ran concurrently with the qualitative data collection. The data was collected using Google Forms, which facilitated the survey. The survey was distributed on social media platforms, with LinkedIn being the primary distribution platform. The target population for the survey was IT, risk, governance, compliance, and other professionals involved in the technology domain within commercial banks in South Africa. Descriptive statistics findings were presented and discussed, followed by CFA analysis.

From the data collected from the literature and the qualitative and quantitative surveys, the researcher concludes that the proposed conceptual framework would support commercial banks in dealing with cyber threats and attacks. The conclusions drawn from information drawn from commercial banks and cybersecurity practitioners showed that cybersecurity within South Africa is a real and present problem. As increased services are offered online, and as the country's threat landscape gets larger, the bigger the prize the government and key infrastructure will present to threat actors across the globe. A concerted effort is required to deal with the challenge. This will require contributions from the government through legislation, building a positive cybersecurity culture in the country, and banks bolstering their capabilities through upskilling, industry-wide information sharing, and technological advancements. The key to upholding a secure posture is to approach cybersecurity holistically (people, process, and technology). Therefore, the author concludes that the study's research objectives were adequately addressed. The key contribution of this thesis was to present a conceptual framework to support commercial banks in mitigating cyber threats and attacks.

References

(ISC)^2. (2021). A Resilient Cybersecurity Profession Charts the Path Forward: (ISC)2 Cybersecurity workforce study, 2021. (ISC)².

(ISC)^2. (2023). Cybersecurity workforce studies A critical need for cybersecurity professionals persists amidst a year of cultural and workplace evolution. (ISC)2.

Abrams, L. (2021, October). Cyberattack shuts down Ecuador's largest bank, Banco Pichincha. Retrieved from Bleepingcomputer.com: https://www.bleepingcomputer.com/news/security/cyberattack-shuts-down-ecuadors-largest-bank-banco-pichincha/

Accenture and Ponemon Institute LLC. (2019). Ninth annual cost of cybercrime study unlocking the value of improved cybersecurity protection. Accenture Security. Accenture. Retrieved from https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf

Accenture South Africa. (2020). Insight into the cyber threat landscape in South Africa. Accenture. Retrieved October 31, 2021, from https://www.accenture.com/za-en/insights/security/cyberthreat-south-africa

Agrafiotis, I., Nurse, J. R., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber-harms: Defining cyber-attacks impacts and understanding how they propagate—Journal of Cybersecurity, 4(1).

Ahmed, M., Sharif, L., Kabir, M., & Al-Maimani, M. (2012, 7). Human Errors in Information Security. International Journal of Advanced Trends in Computer Science and Engineering, 1. Retrieved from http://warse.org/pdfs/ijatcse01132012.pdf

Ajmal, A. B., Shah, M. A., Maple, C., Asghar, M. N., & Islam, S. U. (2021). Offensive Security: Towards Proactive Threat Hunting via Adversary Emulation. IEEE Access, 9, 126023-126033. doi:10.1109/ACCESS.2021.3104260

Albert, B., Tullis, T., & Tedesco, D. (2009). Beyond the usability lab: Conducting large-scale online user experience studies. Morgan Kaufmann.

Albert, D. (2020, October 5). Why Security Can't Live In A Silo. Retrieved June 16, 2022, from Forbes.com: https://www.forbes.com/sites/forbestechcouncil/2020/10/05/why-security-cant-live-in-a-silo/?sh=708372023819

Aldawood, H., & Skinner, G. (2018). Educating and Raising Awareness on Cyber Security Social Engineering: A Literature Review. 2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE), (pp. 66-68).

Alexander, R. D., & Panguluri, S. (2017). Cybersecurity Terminology and Frameworks. In R. M. Clark, & S. Hakim (Eds.), Cyber-Physical Security: Protecting Critical Infrastructure at the State and Local Level (pp. 19–47). Cham: Springer International Publishing. Retrieved from https://doi.org/10.1007/978-3-319-32824-9_2

Allen, B. (2022, June 23). The Ins And Outs Of Insider Threats. Retrieved from Forbes.com: https://www.forbes.com/sites/forbestechcouncil/2022/06/23/the-ins-and-outs-of-insider-threats/?sh=7425bb09eec6

Alshaikh, M. (2020, November). Developing cybersecurity culture to influence employee behavior: A practice perspective. Computers & Security, 98. doi:10.1016/j.cose.2020.102003

Alvesson, M., & Sköldberg, K. (2017). Reflexive Methodology New Vistas for Qualitative Research (Third Edition ed.). SAGE Publications Ltd.

Amissah, M., Gannon, T., & Monat, J. (2020). What is Systems Thinking? Expert Perspectives from the WPI Systems Thinking Colloquium of 2 October 2019. Systems, 8(1).

Aphane, M., & Mofokeng, J. (2021). South African police service capacity to respond to cybercrime: challenges and potentials. Journal of Southwest Jiaotong University, 56(4).

Armstrong, R. C., & Mayo, J. R. (2009). Complexity Science Challenges in Cybersecurity. Argonne.

Babbie, E. (2010). The Practice of Social Research, (Twelfth Edition ed.). Belmont, CA 94002-3098: Wadsworth, Cengage Learning.

Bahl, A., Sharma, A., & Asghar, M. R. (2021). Vulnerability disclosure and cybersecurity awareness campaigns on Twitter during COVID-19. Security and Privacy, 4(6).

Baldassarre, M. T., Barletta, V. S., Caivano, D., & Scalera, M. (2020). Integrating security and privacy in software development. Software Quality Journal, 987-1018.

Banga, G. (2020, November 4). How To Ensure Your NIST Cybersecurity Framework Implementation Isn’t Too Little, Too Late. Retrieved from Forbes: https://www.forbes.com/sites/forbestechcouncil/2020/11/04/how-to-ensure-your-nist-cybersecurity-framework-implementation-isnt-too-little-too-late/?sh=3e3ae4e6364d

Bank for International Settlements and International Organization of Securities Commissions. (2016, June). Committee on Payments and Market Infrastructures Board of the International Organization of Securities Commissions Guidance on cyber resilience for financial market infrastructures. Retrieved November 22, 2021, from https://www.bis.org/cpmi/publ/d146.pdf

Barrett, M. P. (2018). Framework for Improving Critical Infrastructure Cybersecurity Version 1.1

Baykara, M., & Das, R. (2018, August). A novel honeypot-based security approach for real-time intrusion detection and prevention systems. Journal of Information Security and Applications, 41, 103-116. doi:10.1016/j.jisa.2018.06.004

Bell, E., & Bryman, A. (2011). Business Research Methods (3rd ed.). Oxford University Press.

Benya, H., Nan, N., Tanriverdi, H., & Yoo, Y. (2020). Complexity and Information Systems Research in the Emerging Digital World. MIS Quarterly, 44(1), pp. 1-17.

Bert, A. (2018). Three reasons gender diversity is crucial to science. Elsevier Connect.

Bloom, S. (2016). No Vengeance for 'Revenge Porn' Victims: Unraveling Why this Latest Female-Centric, Intimate-Partner Offense is Still Legal, and Why We Should Criminalize It. Fordham Urban Law Journal, 42, 233. Retrieved from https://ir.lawnet.fordham.edu/ulj/vol42/iss1/2

Blum, D. (2020). Rational Cybersecurity for Business: The Security Leaders' Guide to Business Alignment (1 ed.). Berkeley, California: Apress. doi:10.1007/978-1-4842-5952-8

Boehm, J., Curcio, N., Merrath, P., Shenton, L., & Stähle, T. (2019, October 8). The risk-based approach to cybersecurity. Retrieved April 17, 2023, from Mckinsey.com: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-risk-based-approach-to-cybersecurity#/

Boehm, J., Merrath, P., Poppensieker, T., Riemenschnitter, R., & Stähle, T. (2018). Cyber risk measurement and the holistic cybersecurity approach. McKinsey&Company.

Booth, I. (2021, July 28). Transnet cyberattacks could have catastrophic consequences. Retrieved November 16, 2021, from Investec.com: https://www.investec.com/en_za/focus/economy/transnet-cyberattack-could-have-catastrophic-consequences.html

Bote, D. (2019). The South African National Cyber Security Policy Framework: A critical analysis. Potchefstroom: North West University.

Bourgeois, D., Mortati, J., Wang, S., & Smith, J. (2019). Information Systems for Business and Beyond (2019 ed.). Saylor Foundation. Retrieved from https://opentextbook.site/exports/ISBB-2019.pdf

Bramwell, L. (2017, August 21). Parliament of the Republic of South Africa. Retrieved from https://static.pmg.org.za/170822Cybersecurity.pdf

Brantly, A. F. (2019). Conceptualizing cyber policy through complexity theory. Journal of Cyber Policy, 4(2), 275-289.

Brar, H. S., & Kumar, G. (2018). Cybercrimes: A Proposed Taxonomy and Challenges. Journal of Computer Networks and Communications, 2018. doi:10.1155/2018/1798659

Brink, M. (2020, September 04). Get ready to welcome the ‘new banking platform’. Retrieved October 10, 2021, from ITWeb: https://www.itweb.co.za/content/8OKdWMDYeK9qbznQ

Bruce, P., & Bruce, A. (2017). Practical Statistics for Data Scientists: 50 Essential Concepts. O'Reilly Media, Inc.

Bryman, A. (2012). Social research methods (4th Edition ed.). New York: Oxford University Press.

Buckley, J. (2021). The industrialisation of cyber extortion. Computer Fraud & Security, 2021(12), 6-10.

Burrows, T. (2020, August 07). Turn security culture into a value proposition. Retrieved from ITweb: https://www.itweb.co.za/content/nWJad7begXNvbjO1

Business Tech. (2023, July 5). The biggest banks in South Africa in 2023. Retrieved from Businesstech.co.za: https://businesstech.co.za/news/banking/701565/the-biggest-banks-in-south-africa-in-2023/

BusinessTech. (2021). South Africa's best and worst digital banks according to customers. Retrieved October 10, 2021, from https://businesstech.co.za/news/banking/505656/south-africas-best-and-worst-digital-banks-according-to-customers/

Buthelezi, L. (2022, January 24). Hawks arrest Absa engineer for alleged theft of R103 million. Retrieved June 2022, from Fin24: https://www.news24.com/fin24/companies/hawks-arrest-absa-engineer-for-alleged-theft-of-r103-million-20220124

Cabrera, D., & Cabrera, L. (2018). Connecting silos: Solving the problem of organizational silos using a simple systems thinking approach. Cornell University.

Canadian Centre for Cyber Security. (2022). An introduction to Cyber Threat Environment. Ottawa: Communications Security Establishment.

Carter, W. (2017). Forces Shaping the Cyber Threat Landscape for Financial Institutions. SWIFT INSTITUTE. Retrieved from https://ssrn.com/abstract=3047730

Carugi, C. (2014). Analysis through Triangulation and Synthesis to Interpret Data in Mixed Methods Evaluation. In B. o. Health, & I. O. Medicine, Evaluation Design for

Complex Global Initiatives: Workshop Summary (pp. 69-77). Washington: National Academies Press.

Catota, F. E., Morgan, G. M., & Sicker, D. C. (2018, April 30). Cybersecurity incident response capabilities in the Ecuadorian financial sector. Journal of Cybersecurity, 4(1). doi:10.1093/cybsec/tyy002

Center for Internet Security. (2019). CIS Controls V 7.1. Center for Internet Security, Inc.

Chang, W.-J. (2020). Cyberstalking and Law Enforcement. Procedia Computer Science, 176, 1188-1194. doi:10.1016/j.procs.2020.09.115

Chapple, M., Tittel, E., & Stewart, J. M. (2021). CISSP: Certified Information Systems Security Professional Study Guide. Sybex.

Check Point Software Technologies Ltd. (2020, April 20). Coronavirus update: as economic stimulus payments start to flow, cyber-attackers want to get their share, too. Retrieved November 16, 2021, from Check Point Blog: https://blog.checkpoint.com/2020/04/20/coronavirus-update-as-economic-stimulus-payments-start-to-flow-cyber-attackers-want-to-get-their-share-too/

Check Point Software Technologies Ltd. (n.d.). Types of Cyber Attacks. Retrieved November 16, 2021, from Types of Cyber Attacks: https://www.checkpoint.com/cyber-hub/cyber-security/what-is-cyber-attack/types-of-cyber-attacks/#Zero-Day

CheckPoint. (2022). The Different Types of Cybersecurity. Retrieved from Checkpoint.com: https://www.checkpoint.com/cyber-hub/cyber-security/what-is-cybersecurity/

Cheng, Z., Li, Y., Wu, Y., & Luo, J. (2017). The transition from traditional banking to mobile internet finance: an organizational innovation perspective - a comparative study of Citibank and ICBC. Financial Innovation, 12(3).

Chigada, J. (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, No 1(a1194). doi: https://doi.org/10.4102/sajim.v22i1.1194

Chigada, J. (2021). Towards an aligned South African National Cybersecurity Policy Framework. Cape Town.

Chigada, J., & Daniels, N. (2021, September 3). Exploring information systems security implications posed by BYOD for a financial services firm. Business Information Review, 38(3), 115-126.

Chigada, J., & Kyobe, M.E. (2018). Evaluating Factors Contributing to Misalignment of the South African National Cybersecurity Policy Framework. CONF-IRM 2018 Proceedings. 4. Retrieved from https://aisel.aisnet.org/confirm2018/4

Chigada, J., & Madzinga, R. (2021, February 19). Cyberattacks and threats during COVID-19: A systematic literature review. SA Journal of Information Management, 23(1). doi: https://doi.org/10.4102/sajim.v23i1.1277

Chigada, J., & Ngulube, P. (2015). Knowledge-management practices at selected banks in South Africa. South African Journal of Information Management, 17(1), 10.

Cisco. (n.d.). Phishing. Retrieved November 17, 2021, from What Is a Cyberattack?: https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html

Ciso Mag. (2021, September 14). What is Man-in-the-Middle Attack, and How to Prevent them? Retrieved from CISOMag: https://cisomag.com/what-is-man-in-the-middle-attack-and-how-to-prevent-them/

Clarke, V., & Braun, V. (2014). Thematic Analysis. In Encyclopedia of Quality of Life and Well-Being Research. Dordrecht: Springer. doi:https://doi.org/10.1007/978-94-007-0753-5_3470

Clough, J. (2015). Principles of Cybercrime (2nd ed.). Cambridge University Press. doi:https://doi.org/10.1017/CBO9781139540803

Coghlan, D., & Brydon-Miller, M. (2014). The SAGE encyclopedia of action research (Vols. 1-2). London: SAGE Publications Ltd. doi:10.4135/9781446294406

Committee on Payments and Market Infrastructures Board of the International Organization of Securities Commissions. (2016). Guidance on cyber resilience for financial market infrastructures. Bank for International Settlements and International Organization of Securities Commissions.

CompTIA. (2021). What Is a Security Operations Center? Retrieved October 31, 2021, from https://www.comptia.org/content/articles/what-is-a-security-operations-center

Copan, W. G. (2020, February 19). A Conversation on the NIST Privacy Framework. Washington, D.C, Washington.

Cram, W. A., Proudfoot, J. G., & D'Arcy, J. (2020). Maximizing Employee Compliance with Cybersecurity Policies. MIS Quarterly Executive, 19(3), 183-198. doi:10.17705/2msqe.00032

Crawley, K. (2020, May 5). Cybersecurity budgets explained: how much do companies spend on cybersecurity? Retrieved from Cybersecurity ATT: https://cybersecurity.att.com/blogs/security-essentials/how-to-justify-your-cybersecurity-budget

Creswell, J. W. (2015). Research Design: Qualitative, Quantitative, and Mixed Methods Approaches (4th ed.). Sage Publishing Inc.

Creswell, J. W., & Plano Clark, V. L. (2006). Designing and Conducting Mixed Methods Research. Thousand Oaks, CA: Sage.

Creswell, J. W., & Plano Clark, V. L. (2011). Designing and Conducting Mixed Methods Research (2nd ed.). SAGE Publications.

Creswell, J. W., & Plano Clark, V. L. (2017). Designing and Conducting Mixed Methods Research (Third Edition ed.). SAGE Publications, Inc.

Creswell, J. W., & Poth, C. N. (2017). Qualitative Inquiry & Research Design (Fourth Edition ed.). Sage Publication, Inc.

Creswell, J. W., & Tashakkori, A. (2007, January). Editorial: The New Era of Mixed Methods. Journal of Mixed Methods Research, 1(1), 3-7. doi:https://doi.org/10.1177/2345678906293042

Crowd Strike. (2021, October 14). What is phishing? Retrieved from What is a Phishing Attack?: https://www.crowdstrike.com/cybersecurity-101/phishing/

Crowdstrike. (2023, February 28). Threat Actor. Retrieved from Crowdstrike.com: https://www.crowdstrike.com/cybersecurity-101/threat-actor/

Crowson, M. (2020, December). Confirmatory factor analysis using AMOS with CAT Personality Disorder Subscale Data. Confirmatory factor analysis using AMOS with CAT Personality Disorder Subscale Data. Oklahoma.

Cyber Exposure Index. (2021). Country statistics. Retrieved November 14, 2021, from Cyber Exposure Index: https://cyberexposureindex.com/country-statistics/

Cybersecurity & Infrastructure Security Agency. (2007). Defining Computer Security Incident Response Teams. Retrieved October 31, 2021, from https://us-cert.cisa.gov/bsi/articles/best-practices/incident-management/defining-computer-security-incident-response-teams

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

Dawson, C. (2009). Research Methods A practical guide for anyone undertaking a research project (fourth ed.). How To Content.

De Kimpe, L., Walrave, M., Verdegem, P., & Ponnet, K. (2021). What we think we know about cybersecurity: an investigation of the relationship between perceived knowledge, internet trust, and protection motivation in a cybercrime context. Behaviour & Information Technology, 41(8), 1796-1808.

Dekkers, R. (2017). Applied Systems Theory (2nd ed.). Glasgow: Springer.

Deloitte. (2021, February). COVID-19 and the Home Office Balancing Cyber Security and Productivity More staff report that home office IT security hampers productivity. Retrieved from: https://www2.deloitte.com/ch/en/pages/risk/articles/covid-19-home-office-cyber-security.html

Deloitte. (2022). Beneath the surface of a cyberattack, take a deeper look at business impacts. Deloitte.

Deloitte. (2022). Privacy by Design Setting a new standard for privacy certification. Deloitte.

Denzin, N. K. (2015). Triangulation. In The Blackwell Encyclopedia of Sociology.

Denzin, N. K., & Lincoln, Y. S. (2018). The Sage Handbook of Qualitative Research (5th edition ed.). London: Sage.

Department of Justice and Constitutional Development. (2016, December 9). Cybercrimes bill[B 6-2017]. Cybercrimes and cybersecurity bill, Government Gazette No. 40487. Republic of South Africa: Government Gazette No. 40487 of 9 December 2016. Retrieved from https://www.gov.za/documents/cybercrimes-and-cybersecurity-bill-b6-2017-21-feb-2017-0000

Department of Telecommunications and Postal Services. (n.d.). South African National CSIRT 2016. Retrieved March 25, 2023, from Cybersecurity Hub: https://www.cybersecurityhub.gov.za/

Deschenes, E. P. (1990). Longitudinal Research Designs. In K. L. Kempf (Ed.), Measurement Issues in Criminology (pp. 152--166N). New York, NY: Springer, New York. doi:10.1007/978-1-4613-9009-1_7

Dhillon, G. (1997). Managing Information System Security. Macmillan International Higher Education. doi:1.10078/978-1-394-14454-9

Dimensional Research. (2016). Trends in security framework adoption: a survey of it and security professionals. Dimensional Research.

Dlamini, S., & Mbambo, C. (2019). Understanding policing of cybercrime in South Africa: The phenomena, challenges and effective responses. Cogent Social Sciences, 5(1).

Dludla, S. (2021, September 23). SA banks say the latest Debt-IN data breach could have exposed customer data. (IOL) Retrieved October 10, 2021, from IOL: https://www.iol.co.za/business-report/companies/sa-banks-say-latest-debt-in-data-breach-could-have-exposed-customer-data-9ab940a0-6d9e-451e-9a56-7da7a432d57e

Donald, W. E., & Williams, C. K. (2020). Recent Advances and Opportunities for Improving Critical Realism-Based Case Study Research in IS. Journal of the Association for Information Systems, 21(1). doi:10.17705/1jais.00592

Donaldson, S. E., Siegel, S. G., Williams, C. K., Aslam, A., Donaldson, S. E., Siegel, S. G., Aslam, A. (2015). Cybersecurity Frameworks. In Enterprise Cybersecurity: How to Build a Successful Cyberdefense Program Against Advanced Threats (pp. 297–309). Berkeley, CA: Apress. Retrieved from https://doi.org/10.1007/978-1-4302-6083-7_17

Du Toit, R., Hadebe, P. N., & Mphatheni, M. (2018). Public perceptions of cybersecurity: a south african context. Acta Criminologica: Southern African Journal of Criminology, 31(3). Retrieved October 22, 2021, from https://sahs.ukzn.ac.za/wp-content/uploads/2019/07/PUBLIC-PERCEPTIONS-OF-CYBERSECURITY-A-SOUTH-AFRICAN-CONTEXT.pdf

Dupont, B. (2019, September 7). The cyber-resilience of financial institutions: significance and applicability. Journal of Cybersecurity, 1-17. doi:10.1093/cybsec/tyz013

EC-Council. (2021). What is Incident Response? Retrieved November 13, 2021, from Eccounil.org: https://www.eccouncil.org/what-is-incident-response/

Edwards, M. (2020, August 5). Facing the Challenge of Aligning Cybersecurity and Business. Retrieved April 17, 2023, from gca.isa.org: https://gca.isa.org/blog/facing-the-challenge-aligning-cybersecurity-and-business

Emeritus. (2022, November 4). What are Cybersecurity Frameworks and Why Do They Matter? Retrieved March 15, 2023, from Emeritus.org: https://emeritus.org/blog/cybersecurity-what-are-cybersecurity-frameworks/

European Commission. (2007, May 22). European Commission. Retrieved March 27, 2020, from Cybercrime: https://ec.europa.eu/home-affairs/what-we-do/policies/cybercrime_en

European Crime Prevention Network(EUCPN). (2015). Cybercrime: A theoretical overview of the growing digital threat. Retrieved from https://eucpn.org/sites/default/files/document/files/theoretical_paper_cybercrime_.pdf

European Union Agency for Cybersecurity. (2021). Cybersecurity for smes Challenges and Recommendations. ENISA.

European Union Agency for Network and Information Security (ENISA). (2017). Information Sharing and Analysis Centres (ISACs) Cooperative models. ENISA.

European Union Agency for Network and Information Security. (2016). Review of Cyber Hygiene practices. ENISA.

EY Global. (2019, April 09). Cybercrime. What does the most damage, losing data or trust? Retrieved June 16, 2022, from: https://www.ey.com/en_za/financial-services/cybercrime-what-does-the-most-damage-losing-data-or-trust

Ezeji, C. L., Olutola, A. A., & Bello, P. O. (2018). Cyber-related crime in South Africa: extent and perspectives of state's roleplayers. Acta Criminologica: African Journal of Criminology & Victimology, 31(3). doi:10.10520/EJC-14d9dc60ec

Federal Bureau of Investigation. (2020, April 6). Cyber Criminals Conduct Business Email Compromise through Exploitation of Cloud-Based Email Services, Costing US Businesses More Than $2 Billion. Retrieved from scams and safety: https://www.ic3.gov/Media/Y2020/PSA200406

Fin24. (2019). SA banks hit by ransom attacks. Retrieved July 25, 2021, from https://www.news24.com/fin24/companies/financial-services/sa-banks-hit-by-ransom-attacks-minor-disruptions-expected-20191025

Financial Sector Conduct Authority and South African Reserve Bank. (2021). Statement of the need for, intended operation and expected impact of the proposed Joint Standard on financial institutions' cybersecurity and cyber resilience requirements. Pretoria: South African Reserve Bank.

Fischbein, J. (2022, May 10). Insider threats: how the 'Great Resignation' is impacting data security. Retrieved from Weforum.org: https://www.weforum.org/agenda/2022/05/insider-threats-how-the-great-resignation-is-impacting-data-security/

Fortinet. (2021). What is Hacking? | Types of Hacking. Retrieved November 15, 2021, from Fortinet.com: https://www.fortinet.com/resources/cyberglossary/what-is-hacking

Fortinet. (n.d.). What Is Ransomware? Retrieved from Fortinet.com: https://www.fortinet.com/resources/cyberglossary/ransomware

Frey, B. B. (2018). Cluster Sampling. In The SAGE Encyclopedia of Educational Research, Measurement, and Evaluation (Vols. (Vols. 1-4)). Thousand Oaks, CA: SAGE Publications, Inc. doi: https://dx.doi.org/10.4135/9781506326139.n117

Fricker, R. D. (2012). Sampling Methods for Web and E-mail Surveys. In N. Fielding, R. M. Lee, & G. Blank (Eds.), The SAGE Handbook of Online Research Methods (pp. 195-216). London: SAGE Publications. doi:https://dx.doi.org/10.4135/9780857020055.n11

Friedman, B. D., & Allen, K. N. (2014). Systems Theory. In Essentials of Clinical Social Work. Sage publications.

Gandhi, G. (2014). Complexity theory in Cyber Security.

Gartner. (2021). 6 Key Takeaways from the Gartner Board of Directors Survey. Gartner.

Gaumer, Q., Mortier, S., & Moutaib, A. (2016). Financial institutions and cyber crime Between vulnerability and security. Banque de France, Paris.

Gcaza, N., & von Solms, R. (2017). Cybersecurity Culture: An Ill-Defined Problem. IFIP World Conference on Information Security Education, (pp. 98-109).

Gerhardt, M. W., Nachemson-Ekwall, J., & Fogel, B. (2022, March 8). Harnessing the Power of Age Diversity. Retrieved from Harvard Business Review: https://hbr.org/2022/03/harnessing-the-power-of-age-diversity

Given, L. M. (2008). The SAGE encyclopedia of qualitative research methods (Vols. 1-0). Thousand Oaks, CA: SAGE Publications, Inc. doi: 10.4135/9781412963909

Grant, C., & Osanloo, A. (2014). Understanding, Selecting, and Integrating a Theoretical Framework in Dissertation Research: Creating the Blueprint for Your “House”. Administrative issues journal, 4(2).

Greene, J. C. (2007). Mixed Methods in Social Inquiry. San Francisco, California: Jossey-Bass.

Guermazi, B. (2021, August 19). Cybersecurity risks are global. We must address them with a coordinated, collaborative approach. Retrieved from World Bank Blogs: https://blogs.worldbank.org/digital-development/cybersecurity-risks-are-global-we-must-address-them-coordinated-collaborative-approach

Guetzkow, J., Lamont, M., & Mallard, G. (2004). What is Originality in the Humanities and the Social Sciences? American Sociological Review, 69(2), 190-212.

Gundu, T., Flowerday, S., & Renaud, K. (2019). Deliver Security Awareness Training, then Repeat: {Deliver; Measure Efficacy}. 2019 Conference on Information Communications Technology and Society (ICTAS) (pp. 1-6). IEEE.

Hammad, M., Hewahi, N., & Elemdany, W. (2021, March 11). T-SNERF: A novel high accuracy machine learning approach for Intrusion Detection Systems. IET Information Security, 15(2), 178-190. doi:10.1049/ise2.12020

Hatfield, J. M. (2018, March). Social engineering in cybersecurity: The evolution of a concept. Computers & Security, 73, 102-113. doi:10.1016/j.cose.2017.10.008

Hathaway, M., Demchak, C., Kerben, J., McArdle, J., & Spidalieri, F. (2015). CYBER Readiness Index 2.0: a plan for cyber readiness: a baseline and an index. Arlington: Potomac Institute for Policy Studies. Retrieved from https://www.potomacinstitute.org/academic-centers/cyber-readiness-index

Heltman, J. (2016). New York Proposes Cybersecurity Requirements for Banks. American Banker, 181(177).

Hesse-Biber, S. N. (2010). Mixed Methods Research Merging Theory With Practice. New York, NY 10012: The Guilford Press.

Hollard. (2017, January 23). The new word in insurance: cyber insurance. Retrieved June 18, 2022, from Hollard.co.za: https://www.hollard.co.za/brokers/news/short-term-broker-news/the-new-word-in-insurance-cyber-insurance

Huang, K.-J., & Chiang, K.-H. (2021). Toward a Self-Adaptive Cyberdefense Framework in Organization. SAGE Open, 11(1). doi:10.1177/2158244020988855

Hunton, P. (2012). Data attack of the cybercriminal: Investigating the digital currency of cybercrime. Computer Law & Security Review, 28(2), 201-207. doi:https://doi.org/10.1016/j.clsr.2012.01.007

Hwang, I., Wakefield, R., Kim, S., & Kim, T. (2019, August 13). Security Awareness: The First Step in Information Security Compliance Behavior. Journal of Computer Information Systems, 61(4), 345-356.

IBM Cloud Education. (2019, December 4). What are Security Controls? Retrieved June 19, 2022, from ibm.com: https://www.ibm.com/cloud/learn/security-controls

IBM. (2022). Cyber Resilient Organization Study 2021. Retrieved June 16, 2022, from IBM.com: https://www.ibm.com/resources/guides/cyber-resilient-organization-study/

Illidge, M. (2021, October 6). Department of Justice hack — New details emerge. MyBroadBand. Retrieved November 16, 2021, from https://mybroadband.co.za/news/security/417078-department-of-justice-hack-new-details-emerge.html

Insua, D. R., Couce-Vieira, A., Rubio, J. A., Pieters, W., Labunets, K., & Rasines, D. G. (2019). An Adversarial Risk Analysis Framework for Cybersecurity. Risk Analysis, 41(1), 16-36. doi:10.1111/risa.13331

International Monetary Fund. (2022). South Africa financial sector assessment program technical note on cybersecurity risk supervision and oversight. Washington: IMF.

International Organization for Standardization. (n.d.). ISO/IEC 27001 Information security management. Retrieved June 07, 2022, from iso.org: https://www.iso.org/isoiec-27001-information-security.html

INTERPOL. (2020). Global landscape on COVID-19 cyberthreat #WashYourCyberHands. INTERPOL. Retrieved November 16, 2021, from https://www.interpol.int/en/content/download/15217/file/Global%20landscape%20on%20COVID-19%20cyberthreat.pdf

Introna, L., Kavanagh, D., Kelly, S., Orlikowski, W., & Scott, S. (2016). Beyond Interpretivism? New Encounters with Technology and Organization. IFIP WG 8.2 Working Conference on Information Systems and Organizations, IS&O. Dublin.

IOL Media. (2003). How Absa hacker targeted clients' home PCs. Retrieved July 21, 2021, from https://www.iol.co.za/news/south-africa/how-absa-hacker-targeted-clients-home-pcs-110109

IOL Media. (2006). Bank admits to hacking attacks. Retrieved July 21, 2021, from https://www.iol.co.za/news/south-africa/bank-admits-to-hacking-attacks-284319

ISACA. (2013). Transforming Cybersecurity: Using COBIT® 5. ISACA.

ITWeb. (2022, November 16). Cybersecurity Skill Shortage Survey. Retrieved from ITWeb: https://www.itweb.co.za/survey/a1WnxpE74JqV8XLw/content/j5alrvQA6lQvpYQk

Jansen van Vuuren, P. (2002). Environmental scanning – a South African corporate communication perspective with special emphasis on the tertiary sector. PhD Thesis, University of pretoria.

Jarjoui, S., & Murimi, R. (2021). A Framework for Enterprise Cybersecurity Risk Management. In Advances in Cybersecurity Management (pp. 139-161). Springer.

Jeong, J. J., Oliver, G., Kang, E., Creese, S., & Thomas, P. (2021). The current state of research on people, culture and cybersecurity. Personal and Ubiquitous Computing, 25, 809-812. doi:10.1007/s00779-021-01591-8

Johnson, T. P. (2014). Snowball Sampling: Introduction. In N. Balakrishnan, T. Colton, B. Everitt, W. Piegorsch, F. Ruggeri, & J. Teugels (Eds.), Wiley StatsRef: Statistics Reference Online. Wiley Online Library. doi:10.1002/9781118445112.stat05720

Joveda, N., Khan, T., & Pathak, A. (2019, September 17). Cyber Laundering: A Threat to Banking Industries in Bangladesh: In Quest of Effective Legal Framework and Cyber Security of Financial Information. International Journal of Economics and Finance, 11(10). doi:10.5539/ijef.v11n10p54

Joyce, S. (2020). Rethink your cyber budget to get more out of it. PWC.

Jupp, V. (2006). The SAGE dictionary of social research methods (Vols. 1-0). London: Sage Publications. doi:10.4135/9780857020116

Kabanda, G. (2018). A Cybersecurity Culture Framework and Its Impact on Zimbabwean Organizations. Asian Journal of Management, Engineering & Computer Sciences (AJMECS).

Karlsson, F., Hedström, K., & Goldkuhl, G. (2017). Practice-based discourse analysis of information security policies. Computers & Security, 67, 267-279. doi:10.1016/j.cose.2016.12.012.

Kaspersky Lab. (2015). Carbanak apt the great bank robbery. Kaspersky lab. Retrieved from https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08064518/Carbanak_APT_eng.pdf

Kaspersky Lab. (2018). The State of Cyber-Stress: A Study on Americans' and Canadians' Stress levels and mindsets about cybersecurity. Kaspersky Lab.

Kaspersky Labs. (2022). Top Tips for Cyber Hygiene to Keep Yourself Safe Online. Retrieved June 15, 2022, from Kaspersky.com: https://www.kaspersky.com/resource-center/preemptive-safety/cyber-hygiene-habits

Keman, H., & Pearlson, K. (2019, 1). For What Technology Can't Fix: Building a Model of Organizational Cybersecurity Culture. Practice-based IS Research. doi:10.24251/hicss.2019.769

Kline, R. B. (2016). Principles and Practice of Structural Equation Modeling. The Guilford Press.

Klonoff, D. C. (2015, April 16). Cybersecurity for Connected Diabetes Devices. Journal of Diabetes Science and Technology, 9(5), 1143-1147. doi:10.1177/1932296815583334

Knowles, A. (2016, October 12). Tough Challenges in Cybersecurity Ethics. Security Intelligence. Retrieved from https://securityintelligence.com/tough-challenges-cybersecurity-ethics/

Kosutic, D., & Federico, P. (2020). Cybersecurity: investing for competitive outcomes. Journal of Business Strategy, 43(1).

Krishnamurthi, M., Cabrera, D., & Karlovsky, D. (2003). Responsible Conduct in Data Management. Retrieved from https://ori.hhs.gov/education/products/n_illinois_u/datamanagement/dctopic.html#:~:text=Data%20collection%20is%20the%20process,test%20hypotheses%2C%20and%20evaluate%20outcomes.

Kshetri, N. (2019). Cybercrime and Cybersecurity in Africa. Journal of Global Information Technology Management, 22(2), 77-81. doi: 10.1080/1097198X.2019.1603527

Kwak, Y., Damiano, A., & Vishwanath, A. (2020, May). Why do users not report spear-phishing emails? Telematics and Informatics, 48.

Lavrakas, P. J. (2008). Target Population. In Encyclopedia of Survey Research Methods (Vols. 1-0). Thousand Oaks, CA: Sage Publications, Inc. doi: https://dx.doi.org/10.4135/9781412963947.n571

Lazar, J., Feng, J. H., & Hochheiser, H. (2017). Chapter 5 - Surveys. In J. Lazar, J. H. Feng, & H. Hochheiser, Research Methods in Human-Computer Interaction (Second Edition ed., pp. 105-133). Morgan Kaufmann.

Leavy, P. (2017). Research Design Quantitative, Qualitative, Mixed Methods, Arts-Based, and Community-Based Participatory Research Approaches. New York: The guilford press. Retrieved September 08, 2021

Lee, C. S., & Kim, D. (2022, February 03). Pathways to Cybersecurity Awareness and Protection Behaviors in South Korea. Journal of Computer Information Systems, 63(1), 94-106.

Lee, J. (2020). Statistics, Descriptive. International Encyclopedia of Human Geography, 13-20.

Lee, L. (2019). Cybercrime has evolved: it's time cyber security did, too. Computer Fraud & Security, 2019(6), 8-11.

Lee, M., & Schuele, M. (2010). Demographics. In Encyclopedia of Research Design (Vols. 1-0). Sage Publications, Inc.

Leedy, P. D. (2010). Practical research: planning and design (9th ed. ed.). Boston: Pearson.

Leedy, P. D., & Ormond, J. E. (2016). Practical research: planning and design (Eleventh ed.). Pearson.

Lennartsson, M., Kävrestad, J., & Nohlberg, M. (2021). Exploring the meaning of usable security – a literature review. Information and Computer Security, 29(4).

Lester, J. N., Cho, Y., & Lochmiller, C. R. (2020). Learning to Do Qualitative Data Analysis: A Starting Point. Human Resource Development Review, 19(1), 94-106.

Levy, D. L. (2000). Applications and Limitations of Complexity Theory in Organization Theory and Strategy.

Levy, P. S. (2014). Cluster Sampling. In Wiley StatsRef: Statistics Reference Online. John Wiley & Sons. doi:10.1002/9781118445112.stat05694

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

Littlejohn, S. W., & Foss, K. A. (2009). Axiology. In S. W. Littlejohn, & K. A. Foss (Eds.), Encyclopedia of communication theory (Vol. 1, pp. 70-74). SAGE Publications, Inc. doi: 10.4135/9781412959384.n27

Lockheed Martin Corporation. (2011). Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. (E. M. Hutchins, M. J. Cloppert, & R. M. Amin, Eds.) Retrieved from https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf.

Mabunda, S. (2019, June). Cyber Extortion, Ransomware and the South African Cybercrimes and Cybersecurity Bill. Statute Law Review, 40(2), 143-154. doi:10.1093/slr/hmx028

Madey, D. L. (1982). Some Benefits of Integrating Qualitative and Quantitative Methods in Program Evaluation with Illustrations. Educational Evaluation and Policy Analysis, 223-236. doi:10.3102/01623737004002223

Malatras, A., Skouloudi, C., & Koukounas, A. (2019). Industry 4.0 cybersecurity: challenges & recommendations. European Union Agency for Network and Information Security

(ENISA). European Union Agency for Network and Information Security (ENISA): European Union Agency for Network and Information Security (ENISA). doi:10.2824/143986

Malhotra, N. K., Nunan, D., & Birks, D. F. (2017). Marketing Research An Applied Approach (Fifth ed.). Edinburgh: Pearson.

Malinga, S. (2021, September 03). SA tech firms strive to disrupt the gender status quo. Johannesburg, Gauteng, South Africa: ITWeb.

Malwarebytes. (2021). Hacking. Retrieved November 15, 2021, from Malwarebytes.com: https://www.malwarebytes.com/hacker

Marble, J. L., Lawless, W. F., Mittu, R., Coyne, J., Abramson, M., & Sibley, C. (2015). In Cyber Warfare: Building the Scientific Foundation (pp. 173–206). Cham. doi:10.1007/978-3-319-14039-1_9

Marchetti, M., Colajanni, M., Messori, M., Aniello, L., & Vigfusson, Y. (2012). Cyber Attacks on Financial Critical Infrastructures. In R. Baldoni, & G. Chockler (Eds.), Collaborative Financial Infrastructure Protection: Tools, Abstractions, and Middleware (pp. 53–82). Berlin, Heidelberg: Springer Berlin Heidelberg. Retrieved from https://doi.org/10.1007/978-3-642-20420-3_3

Marr, B. (2018, September 2). What is Industry 4.0? Here's A Super Easy Explanation For Anyone. Forbes. Retrieved October 24, 2021, from https://www.forbes.com/sites/bernardmarr/2018/09/02/what-is-industry-4-0-heres-a-super-easy-explanation-for-anyone/?sh=3196e92a9788

Martins, A., & Eloff, J. (2002). Information Security Culture. In A. M. Ghonaimy, M. T. El-Hadidi, & H. K. Aslan (Eds.), Security in the Information Society: Visions and Perspectives (pp. 203-214). Boston: Springer. doi:10.1007/978-0-387-35586-3_16

Mathison, S. (2005). Encyclopedia of Evaluation. Sage Publications Inc.

Mbelli, T. M., & Dwolatzky, B. (2016, 6). Cyber Security, a Threat to Cyber Banking in South Africa: An Approach to Network and Application Security. 2016 IEEE 3rd

International Conference on Cyber Security and Cloud Computing (CSCloud), (pp. 1-6). doi:10.1109/CSCloud.2016.18

McBride, N. (2005, May 26). Chaos theory as a model for interpreting information systems in organizations. Information Systems Journal, 15(3), 233-254.

McKane, J. (2019). South African banks hit by massive DDoS attack. Retrieved July 25, 2021, from https://mybroadband.co.za/news/banking/324881-south-african-banks-hit-by-massive-ddos-attack.html

McLeod, A., Dorantes, C. A., & Dietrich, G. (2008). Modeling Security Vulnerabilities Using Chaos Theory: Discovering Order, Structure, and Patterns from Chaotic Behavior in Complex Systems. 7th Annual Security Conference.

Merriam-Webster dictionary. (2023, January 17). Complexity theory. Merriam-Webster.

Metz, T. (2011). Ubuntu as a moral theory and human rights in South Africa. African Human Rights Law Journal, 11(2), 235-559. Retrieved October 22, 2021, from https://www.ahrlj.up.ac.za/metz-t

Minnaar, A. (2020). ‘Gone phishing’: the cynical and opportunistic exploitation of the Coronavirus pandemic by cybercriminals. Acta Criminologica: African Journal of Criminology & Victimology, 33(3). doi:10.10520/ejc-crim-v33-n3-a3

Mitnick, K. D., Simon, W. L., & Wozniak, S. (2002). The Art of Deception: Controlling the Human Element of Security. Wiley.

Mohamad, M. M., Sulaiman, N. L., Sern, L. C., & Salleh, K. M. (2015). Measuring the Validity and Reliability of Research Instruments. 4th World Congress on Technical and Vocational Education and Training (WoCTVET). 204, pp. 164-171. ScienceDirect.

Mokobane, N. B., & Botha, R. A. (2020). Does Ubuntu Influence Social Engineering Susceptibility? In N. Clarke, & S. Furnell (Eds.), Human Aspects of Information Security and Assurance (Vol. 593, pp. 97--108). Cham: Springer International Publishing. doi:10.1007/978-3-030-57404-8_8

Möller, D. P. (2020). Introduction to Digital Transformation. In Cybersecurity in Digital Transformation. Springer, Cham. doi:10.1007/978-3-030-60570-4_1

Morse, J., Barrett, M., Mayan, M., Olson, K., & Spiers, J. (2002). Verification Strategies for Establishing Reliability and Validity in Qualitative Research. International Journal of Qualitative Methods, 1(2), 13-22.

Mossburg, E., Gelinne, J., & Calzada, H. (2016). Beneath the surface of a cyberattack: A deeper look at business impacts. Deloitte Advisory. Deloitte. Retrieved from https://www2.deloitte.com/us/en/pages/risk/articles/hidden-business-impact-of-cyberattack.html

Mothibi, k., & Amali, S. E. (2018, September). Curbing cybercrime at institutions of higher learning: a case study of the Information Communication Technology unit (ICT) at selected South African universities. Acta Criminologica: African Journal of Criminology & Victimology, 31(8). doi:10.10520/EJC-14d8fee33e

Moyo, A. (2016). Standard Bank heist modus operandi 'not new'. Retrieved July 25, 2021, from https://www.itweb.co.za/content/nkLgB1MeNZGq59N4

Moyo, B. (2018). An analysis of competition, efficiency and soundness in the South African banking sector. South African Journal of Economic and Management Sciences, 21(1)(a2291). doi: 10.4102/sajems.v21i1.2291

Mueller, R., & Hancock, G. (2001). Factor Analysis and Latent Structure, Confirmatory Author links open overlay panel. In International Encyclopedia of the Social & Behavioral Sciences (pp. 5239-5244). Oxford: Pergamon.

Musoni, M. (2019, July 9). The criminalization of "Revenge Porn" in South Africa. Obiter, 40(1). doi:10.10520/EJC-16cc6d96a4

Mutemwa, M., Mtsweni, J., & Mkhonto, N. (2017). Developing a Cyber Threat Intelligence sharing platform for South African Organisations. 2017 Conference on Information Communications Technology and Society (ICTAS), (pp. 1-6). Durban.

My Broadband. (2022, March 20). TransUnion faces R10-million fine for hack. Retrieved June 18, 2022, from mybroadband.com:

https://mybroadband.co.za/news/security/438098-transunion-faces-r10-million-fine-for-hack.html

MyBroadBand. (2021, October 03). Hackers steal R100 million from South African University — but lost most of it. MyBroadBand. Retrieved November 16, 2021, from https://mybroadband.co.za/news/security/416742-hackers-steal-r100-million-from-south-african-university-but-lost-most-of-it.html

Myers, M. D. (2019). Qualitative Research in Business and Management (third edition ed.). London: SAGE Publications Ltd.

Naidoo, S. (2021, July 27). Transnet cyber attack confirmed: Port terminals division declares force majeure. (Moneyweb, Producer) Retrieved October 10, 2021, from Moneyweb: https://www.moneyweb.co.za/news/companies-and-deals/transnet-cyber-attack-confirmed-port-terminals-division-declares-force-majeure/

National Association of Geoscience Teachers. (2017). Analysis Tools. Retrieved June 22, 2021, from https://nagt.org/nagt/geoedresearch/toolbox/analysis_tools/index.html

National Institute of Standards and Technology. (2018, July). Uses and Benefits of the Cybersecurity Framework.

National Institute of Standards and Technology. (2019). Information security - Glossary | CSRC. information security - Glossary | CSRC. National Institute of Standards and Technology. Retrieved from https://csrc.nist.gov/glossary/term/information_security

National Institute of Standards and Technology. (n.d.). Man-in-the-middle attack (MitM). Retrieved November 17, 2021, from Information Technology Laboratory Computer security resource center: https://csrc.nist.gov/glossary/term/man_in_the_middle_attack

Nedbank. (2020). Nedbank warns clients of the potential impact of data incident at Computer Facilities (Pty) Ltd. Retrieved August 14, 2021, from https://www.nedbank.co.za/content/nedbank/desktop/gt/en/info/campaigns/nedbank-warns-clients.html

Newman, D. (2017, January 24). How To Drive Productivity Without Compromising Cybersecurity. Retrieved from Forbes.com: https://www.forbes.com/sites/danielnewman/2017/01/24/how-to-drive-productivity-without-compromising-cybersecurity/?sh=57e376dd793d

News24Wire. (2016). Standard Bank computer was hacked in R300 million ATM fraud hit. Retrieved July 25, 2021, from https://businesstech.co.za/news/banking/128602/standard-bank-computer-was-hacked-in-r300-million-atm-fraud-hit/

Nielsen, M. W., Alegria, S., Börjeson, L., Etzkowitz, H., Falk-Krzesinski, H. J., Joshi, A.,... Schiebinger, L. (2017). Gender diversity leads to better science. Proceedings of the National Academy of Sciences, 114, 1740-1742.

Northern Ireland Cyber Security Centre. (2023, February 28). Cyber Threats. Retrieved from nicybersecuritycentre.gov.uk: https://www.nicybersecuritycentre.gov.uk/cyber-threats

Ntsaluba, N. (2017). Cybersecurity policy and legislation in South Africa. Pretoria: University of Pretoria.

O'Sullivan, E., Rassel, G., Berner, M., & DeVance Taliaferro, J. (2017). Research Methods for Public Administrators (Sixth Edition ed.). New York, NY 10017: Routledge.

Ocholla, D. N., & Le Roux, J. (2011). Conceptions and misconceptions of theoretical frameworks in library and information science research: a case study of selected theses and dissertations from eastern and southern African universities. Mousaion: South African Journal of Information Studies, 61-74.

Oiaga, M. (2006). Three South African Banks Hit by Hackers. Retrieved July 21, 2021, from https://news.softpedia.com/news/Three-South-African-Banks-Hit-by-Hackers-28590.shtml

Olkin, I., & Sampson, A. (2001). Multivariate Analysis: Overview. International Encyclopedia of the Social & Behavioral Sciences, 10240-10247. doi 10.1016/B0-08-043076-7/00472-1.

Onwuegbuzie, A. J., & Leech, N. L. (2005). On Becoming a Pragmatic Researcher: The Importance of Combining Quantitative and Qualitative Research Methodologies. International Journal of Social Research Methodology, 8, 375-387. doi:10.1080/13645570500402447

Open Group Standard. (2017). Open Information Security Management Maturity Model (O-ISM3), Version 2.0. The Open Group.

Padayachee, R., & Pillay, V. (2018, April 18). Women remain under-represented in emerging tech. PwC South Africa.

Parent, M., & Cusack, B. (2016). Cybersecurity in 2016: People, technology, and processes. Business Horizons, 59(6), 567-569.

Parker, C., Scott, S., & Geddes, A. (2019). Snowball Sampling. London: SAGE Publications, Inc.

Parsons, V. L. (2017, February 15). Stratified Sampling. Wiley StatsRef: Statistics Reference Online. doi: 10.1002/9781118445112.stat05999.pub2

Payment Card Industry Data Security Standard. (2022). Requirements and Testing Procedures, v4.0. PCI Security Standards Council.

Payne, G., & Payne, J. (2004). Evaluation Studies. In Key Concepts in Social Research. SAGE Publications, Ltd. doi: 10.4135/9781849209397.n16

Petersen, F. (2019). Determinants for the acceptance and use of mobile health applications: Diabetic patients in the Western Cape, South Africa. University of the Western Cape.

Pfleeger, S. L., & Caputo, D. D. (2012). Leveraging behavioral science to mitigate cyber security risk. Computers & Security, 31(4), 597-611. doi: 10.1016/j.cose.2011.12.010.

Pituch, K. A., & Stevens, J. P. (2016). Applied Multivariate Statistics for the Social Sciences Analyses with SAS and IBM’s SPSS, Sixth Edition. Routledge.

Plotnek, J. J., & Slay, J. (2021, March). Cyber terrorism: A homogenized taxonomy and definition. Computers & Security, 102. doi:10.1016/j.cose.2020.102145

Potgieter, D. W. (2011). Absa intercepts Land Bank swindle. Retrieved July 21, 2021, from https://www.iol.co.za/business-report/companies/absa-intercepts-land-bank-swindle-1009423

Price Waterhouse Coopers. (2022). Using upskilling to solve the cybersecurity talent shortage. ProEdge.

Rahman, M. M. (2021, February 9). Essential Cybersecurity Components: Continuous Monitoring, Human Intelligence and Commitment. Retrieved from ISACA Now Blog: https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2021/essential-cybersecurity-components-continuous-monitoring-human-intelligence-and-commitment

Rama, P., & Keevy, M. (2022). A comparative review of South Africa's government-led cybersecurity awareness measures to those of world-leading countries. Southern African Journal of Accountability and Auditing Research, 117-128.

Ramluckan, T., van Niekerk, B., & Leenen, L. (2020). Cybersecurity and information warfare research in South Africa: Challenges and proposed solutions. Journal of Information Warfare, 19(1), 80-95. Retrieved October 31, 2021, from https://www.jinfowar.com/journal/volume-19-issue-1/cybersecurity-information-warfare-research-south-africa-challenges-proposed-solutions

Rao, R. H., & Herath, T. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. Behavioral and Policy Issues in Information Systems Security, 18(2), 106-125. doi:10.1057/ejis.2009.6

Raphael, J. J., Célestin, J. C., & Djiethieu, E. R. (2019, September 9). A Key to Strengthening IT Security? Chaos.

Rassel, G., Leland, S., Mohr, Z., & O'Sullivan, E. (2020). Research Methods for Public Administrators (7th Edition ed.). Routledge.

Ratten, V. (2019, September 23). The effect of cybercrime on open innovation policies in technology firms. Information Technology & People, 32(5), 1301-1317. doi:10.1108/ITP-03-2018-0119

Reinking, D., & Alvermann, D. E. (2005). Editorial: What Are Evaluation Studies, and Should They Be Published in "RRQ"? Reading Research Quarterly, 40. Retrieved from http://www.jstor.org/stable/4151677

Republic of South Africa. (2013, November 26). No.4 of 2013: Protection of Personal Information Act, 2013. Retrieved October 21, 2021, from https://www.gov.za/sites/default/files/gcis_document/201409/3706726-11act4of2013popi.pdf

Republic of South Africa. (2013). Protection of Personal Information Act. Cape Town, Republic of South Africa: Parliament of the Republic of South Africa.

Republic of South Africa. (2015, December 4). National Cybersecurity Policy Framework. Retrieved October 22, 2021, from https://www.gov.za/sites/default/files/gcis_document/201512/39475gon609.pdf

Republic of South Africa. (2021, June 1). Cybercrimes Act 19 of 2020. Retrieved October 21, 2021, from https://www.gov.za/sites/default/files/gcis_document/202106/44651gon324.pdf

Reva, D. (2021, July 29). Cyber attacks expose the vulnerability of South Africa's ports. Retrieved November 16, 2021, from Institute for Security Studies: https://issafrica.org/iss-today/cyber-attacks-expose-the-vulnerability-of-south-africas-ports

Revicki, D. (2014). Internal Consistency Reliability. In Encyclopedia of Quality of Life and Well-Being Research (pp. 3305-3306). Springer, Dordrecht.

Rossman, G. B., & Rallis, S. F. (2017). An Introduction to Qualitative Research (Fourth Edition ed.). Sage.

Ruel, E., Wagner III, W. E., & Gillespie, B. J. (2016). The Practice of Survey Research: Theory and Applications. Thousand Oaks, CA: SAGE Publications, Inc. doi:10.4135/9781483391700

SABRIC. (2023). Information Manual. SABRIC. Johannesburg: Sabric.

Salim, H., & Madnick, S. (2016). Cyber Safety: A Systems Theory Approach to Managing Cyber Security Risks – Applied to TJX Cyber Attack. Massachusetts: Massachusetts Institute of Technology.

Salkind, N. J. (2010). Encyclopedia of research design (Vols. 1-0). Thousand Oaks, California: SAGE Publications, Inc. doi:10.4135/9781412961288

Salkind, N. J. (2012). Exploring Research (Eighth Edition ed.). Pearson.

Sanders, R. (2016). Embedding Cyber-security into Your Company's DNA. People & Strategy, 39(1), 8-9.

SANS Institute. (2019). 2019 SANS Security Awareness Report. SANS Institute.

SANS Institute. (2021, November 23). Security Awareness Metrics – What to Measure and How. Retrieved from Sans.org: https://www.sans.org/blog/security-awareness-metrics-what-to-measure-and-how/

SANS. (2021). 2021 Security awareness report managing human cyber risk. SANS Institute.

Sarmento, R., & Costa, V. (2019). Confirmatory Factor Analysis A Case Study. Porto: Faculty of Engineering - Univesity of Porto.

SAS Institute Inc. (2013, December). SAS/STAT® 13.1 User's Guide. Retrieved August 22, 2021, from https://support.sas.com/documentation/onlinedoc/stat/131/introsamp.pdf

Saunders, B., Sim, J., Kingstone, T., Baker, S., Waterfield, J., Bartlam, B.,... Jinks, C. (2018). Saturation in qualitative research: exploring its conceptualization and operationalization. Qual Quant, 54(2), 1893-1907. doi:10.1007/s11135-017-0574-8

Saunders, M. N., Lewis, P., & Thornhill, A. (2019). Research Methods For Business Students (Eighth ed.). Pearson Education Limited.

Savage, S., & Schneider, F. B. (2009). Security is Not a Commodity: The Road Forward for Cybersecurity Research. Washington: Computer Science & Telecommunications Board of the National Research Council.

Schwab, K. (2015, December 12). The Fourth Industrial Revolution: What It Means and How to Respond. Foreign Affairs. Retrieved October 24, 2021, from https://www.foreignaffairs.com/articles/2015-12-12/fourth-industrial-revolution

Schwab, K. (2017). The Global Competitiveness Report 2017-2018. Geneva: World Economic Forum.

Schwab, K. (2019). The Global Competitiveness Report 2019. Geneva: World Economic Forum.

Shaked, A., Tabansky, L., & Reich, Y. (2021). Incorporating Systems Thinking Into a Cyber Resilience Maturity Model. IEEE Engineering Management Review, 49(2), 110-115.

Sicetsha, A. (2018, September 17). SAPS cybercrime unit unable to function due to expired software licenses. Retrieved from Thesouthafrican.com: https://www.thesouthafrican.com/news/saps-cybercrime-unit-expired-software-license/

Simbanegavi, W., Greenberg, J. B., & Gwatidzo, T. (2015). Testing for Competition in the South African Banking Sector. Journal of African Economies, 24(3), 303-324. doi:10.1093/jae/eju022

Sinnot, J. D., & Rabin, J. S. (2012). Sex Roles. In Encyclopedia of Human Behavior (Second Edition ed., pp. 411-417). Academic Press.

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

Siponen, M. T., Mahmood, A. M., & Pahnila, S. (2014, March). Employees' adherence to information security policies: An exploratory field study. Information & Management, 51(2), 217-224.

Smith, A. (2004). Complexity Theory as a Practical Management Tool: A Critical Complexity Theory as a Practical Management Tool: A Critical Evaluation. Organization Management Journal Organization Management Journal, 1(2).

Smith, K. T., Jones, A., Johnson, L., & Smith, L. M. (2019). Examination of cybercrime and its effects on corporate stock value. Journal of Information, Communication and Ethics in Society, 17(1), 42-60. doi:10.1108/JICES-02-2018-0010

Smith, Z. M., & Lostri, E. (2020). The Hidden Costs of Cybercrime. McAfee. Retrieved November 18, 2021, from https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf

South African Banking Risk Information Centre (SABRIC). (2019). Annual Crime Stats 2019. Johannesburg: South African Banking Risk Information Centre (SABRIC).

South African Banking Risk Information Centre (SABRIC). (2023). Identity Theft. Retrieved April 16, 2023, from Sabric.co.za: https://www.sabric.co.za/stay-safe/identity-theft/

South African Banking Risk Information Centre (SABRIC). (n.d.). Cybercrime. Retrieved April 18, 2023, from Sabric.co.za: https://www.sabric.co.za/stay-safe/cybercrime/

South African Banking Risk Information Centre (SABRIC). (n.d.). Cybersecurity. Retrieved April 18, 2023, from Pmg.org.za: https://pmg.org.za/files/170228SABRIC-Cybersecurity.pptx

South African Reserve Bank Prudential Authority. (2020). Prudential Authority Annual Report 2019/2020. Pretoria: South African Reserve Bank Prudential Authority. Retrieved October 5, 2021, from https://www.resbank.co.za/en/home/publications/publication-detail-pages/reports/pa-annual-reports/2020/10227

South African Reserve Bank. (2020, October 8). South African Reserve Bank imposes administrative sanctions on banks. Retrieved June 18, 2022, from Resbank.co.za: https://www.resbank.co.za/en/home/publications/publication-detail-pages/media-releases/2016/7425

Srinidhi, B., Yan, J., & Tayi, G. K. (2015, July). Allocation of resources to cyber-security: The effect of misalignment of interest between managers and investors. Decision Support Systems, 75, 49-62.

Srinivas, J., Das, A. K., & Kumar, N. (2019, March). Government regulations in cyber security: Framework, standards and recommendations. Future Generation Computer Systems, 92, 178-188.

Stackpole, B. (2022, March 15). How to build a culture of cybersecurity. Retrieved from MIT Sloan: https://mitsloan.mit.edu/ideas-made-to-matter/how-to-build-a-culture-cybersecurity

Stake, R. E. (1995). The Art of Case Study Research. Sage.

Stratton, S. J. (2021). Population Research: Convenience Sampling Strategies. Prehospital and disaster medicine, 36(4), 373-374.

Such, J. M., Ciholas, P., Rashid, A., Vidler, J., & Seabrook, T. (2019). Basic Cyber Hygiene: Does It Work? Computer, 52(4), 21-31.

Sue, V. M., & Ritter, L. A. (2012). Conducting Online Surveys (2nd Edition ed.). Sage. doi:10.4135/9781506335186.n1

Suhr, D. D. (2005). Exploratory or Confirmatory Factor Analysis? SUGI 30 Proceedings. Philadelphia: SAS.

Sutherland, E. (2017). Governance of Cybersecurity – The Case of South Africa. The African Journal of Information and Communication (AJIC), 20, 83-112.

Swart, W., & Wa Afrika, M. (2012). It was a happy New Year's Day for gang who pulled off...R42m Postbank heist. Retrieved July 21, 2021, from https://www.timeslive.co.za/news/south-africa/2012-01-15-it-was-a-happy-new-years-day-for-gang-who-pulled-offr42m-postbank-heist/

Syed, R. (2020). Cybersecurity vulnerability management: A conceptual ontology and cyber intelligence alert system. Information & Management, 57(6). doi:10.1016/j.im.2020.103334

Taddeo, M. (2012). An analysis for just cyber warfare in Cyber Conflict (CYCON). 2012 4th International Conference on, (pp. 1-10).

Tavakol, M., & Dennick, R. (2011, June 27). Making sense of Cronbach's alpha. International Journal of Medical Education, 53-55.

Tavakol, M., & Wetzel, A. (2020). Factor Analysis: A means for theory and instrument development in support of construct validity. International Journal of Medical Education, 11, 245-247.

Teddlie, C., & Tashakkori, A. (2008). Foundations of Mixed Methods Research Integrating Quantitative and Qualitative Approaches in the Social and Behavioral Sciences. SAGE Publications, Inc.

Teddlie, C., & Yu, F. (2007). Mixed Methods Sampling: A Typology With Examples. Journal of Mixed Methods Research, 1(1), 77-100. doi: 10.1177/1558689806292430.

Teichmann, M. (2020, October). Cybersecurity: a holistic approach to business resilience. Retrieved April 17, 2023, from Accenture.com: https://www.accenture.com/nl-en/blogs/insights/cybersecurity-holistic-approach-to-cyber-resilience

The information regulator of South Africa. (2021, April 1). Protection of Personal Information Act, 2013 (act no. 4 of 2013). Retrieved October 21, 2021, from https://www.gov.za/sites/default/files/gcis_document/202104/44383gon297.pdf

The International Telecommunications Union. (2017). Definition of cybersecurity. Retrieved 04 11, 2020, from https://www.itu.int/en/ITU-T/studygroups/2013-2016/17/Pages/cybersecurity.aspx

The Open Group. (2011). Open Information Security Management Maturity Model (O-ISM3). The Open Group. Reading: The Open Group.

Thompson, W., & Farber, T. (2020). Absa says 'some sensitive customer information' stolen by employee. Retrieved August 14, 2021, from https://www.timeslive.co.za/sunday-times/business/2020-12-01-absa-says-some-sensitive-information-leaked-by-employee/

Thompson. (2020). Threat Intelligence. In E. C. Thompson, Designing a HIPAA-Compliant Security Operations Center. Berkeley: Apress. doi:10.1007/978-1-4842-5608-4_3

Tisdale, S.M. (2015). Cybersecurity: Challenges From a Systems, Complexity, Knowledge Management and Business Intelligence Perspective. Issues in Information Systems, 16(III), 191-198. Retrieved from https://www.semanticscholar.org/paper/Cybersecurity%3A-Challenges-From-a-Systems%2C-Knowledge-Tisdale/5e0bb009f7b87d3fff87b20e156a56a726f891fb

Toyana, M. (2021, September 13). Hack attack: Department of Justice and SA Space Agency say no ransom demands made after IT breaches. Daily Maverick. Retrieved November 16, 2021, from https://www.dailymaverick.co.za/article/2021-09-13-hack-attack-department-of-justice-and-sa-space-agency-say-no-ransom-demands-made-after-it-breaches/

Tredger, C. (2023, March 24). Lack of skills and an immature judicial system weaken SA's cyber security stance. Retrieved from ITWeb: https://www.itweb.co.za/content/LPwQ57lbNwkqNgkj

Trend Micro. (2016, July 19). Ransom Notes: Know What Ransomware Hit You. Retrieved November 17, 2021, from Ransom Notes: Know What Ransomware Hit You: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransom-notes-know-what-ransomware-hit-you

Turner, J. R., & Baker, R. M. (2019, January 10). Complexity Theory: An Overview with Potential Applications for the Social Sciences. Systems, 7(1).

Uchendu, B., Nurse, J. R., Bada, M., & Furnell, S. (2021, October). Developing a cyber security culture: Current practices and future needs. Computers & Security, 109.

United Nations. (n.d.). Global Programme on Cybercrime. Retrieved November 13, 2022, from Unodc.org: https://www.unodc.org/unodc/es/cybercrime/global-programme-cybercrime.html

Van der Kleij, R., Schraagen, J. M., Cadet, B., & Young, H. (2022, February). Developing decision support for cybersecurity threat and incident managers. Computers & Security, 113. doi:10.1016/j.cose.2021.102535

Van der Kleut, J. (2021). Identity theft: What is it and how to avoid it. Retrieved November 15, 2021, from Norton.com: https://us.norton.com/internetsecurity-id-theft-what-is-identity-theft.html

Van der Westhuizen, H. (2019, 6). New Bill offers a robust game plan against cybercrime in South Africa | SAIIA. New Bill offers a robust game plan against cybercrime in South Africa | SAIIA.

Van Niekerk, B. (2017). An Analysis of Cyber-Incidents in South Africa. The African Journal of Information and Communication (AJIC), 20, 113-132. doi: 10.23962/10539/23573

Van Niekerk, J., & von Solms, R. (2013). Using Bloom's Taxonomy for Information Security Education. Information Assurance and Security Education and Training. WISE 2013, WISE 2011, WISE 2009. 406, pp. 280-287. Springer. doi: 10.1007/978-3-642-39377-8_33

Van Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. Computers & Security, 38, 97-102. doi: 10.1016/j.cose.2013.04.004

Vaus, D. D. (2001). Research Design in Social Research (First Edition ed.). SAGE Publications Ltd.

Vecchiatto, P. (2003). Hack not to blame in new Absa fraud case. Retrieved July 21, 2021, from https://www.itweb.co.za/content/mYZRX79PaepvOgA8

Venter, I. M., Blignaut, R. J., Renaud, K., & Venter, M. A. (2019, December). Cyber security education is as essential as “the three R's”. Heliyon, 5(12).

Vermeulen, J. (2021, September 8). South African space agency hit by data breach. Retrieved from Mybroadband.co.za: https://mybroadband.co.za/news/security/413124-south-african-space-agency-hit-by-data-breach.html

Von Solms, B. (2022, September 26). Five things South Africa must do to combat cybercrime. Retrieved from Daily Maverick:

https://www.dailymaverick.co.za/article/2022-09-26-five-things-south-africa-must-do-to-combat-cybercrime/

Wang, S., Ding, L., Sui, H., & Gu, Z. (2021). Cybersecurity risk assessment method of ICS based on attack-defense tree model. Journal of Intelligent & Fuzzy Systems, 40(6), 10475-10488.

Wells, L. J., Camelio, J. A., Williams, C. B., & White, J. (2014). Cyber-physical security challenges in manufacturing systems. Manufacturing Letters, 2, 74-77. doi:10.1016/j.mfglet.2014.01.005

Whateley, C. (2021, March 23). Is platform banking the right strategy for South Africa? (Accenture South Africa) Retrieved October 10, 2021, from https://southafricablog.accenture.com/is-platform-banking-the-right-strategy-for-south-africa

Wilholt, T. (2009). Bias and values in scientific research. Studies in History and Philosophy of Science Part A, 40, 92-101. doi: 10.1016/j.shpsa.2008.12.005

Wilkinson, L. A. (2011). Systems Theory. Encyclopedia of Child Behavior and Development, pp. 1466-1468.

Winjit. (2021, March 31). Why SA businesses need to consider cyber security. Why SA businesses need to consider cyber security. Retrieved October 31, 2021, from https://www.itweb.co.za/content/Kjlyr7w14BEqk6am

Wood, C. C. (2008). Information Security Policies Made Easy. InformationShield.

World Economic Forum. (2019, November 1). Why good cybersecurity in business is everyone’s responsibility. (P. H. Adams, Producer) Retrieved from Weforum.org: https://www.weforum.org/agenda/2019/11/cybersecurity-best-practice-business/

World Economic Forum. (2020). COVID-19 Risks Outlook A Preliminary Mapping and Its Implications. Cologny/Geneva: World Economic Forum. Retrieved November 16, 2021,from https://www3.weforum.org/docs/WEF_COVID_19_Risks_Outlook_Special_Edition_Pages.pdf

World Economic Forum. (2022, 03 10). Can closing the cybersecurity skills gap change the world? Retrieved from Weforum.org: https://www.weforum.org/agenda/2022/03/closing-the-cybersecurity-skills-gap/#:~:text=Despite%20the%20headlines%20we've,year%2C%20it's%20simply%20not%20enough.

World Economic Forum. (2023, February 1). Cybersecurity: How closing the skills gap can improve resilience and support a workforce in transition. Retrieved from Weforum.org: https://www.weforum.org/agenda/2023/02/cybersecurity-how-to-improve-resilience-and-support-a-workforce-in-transition/

World Health Organization. (2020, March 11). WHO Director-General's opening remarks at the media briefing on COVID-19 - 11 March 2020. Retrieved November 16, 2021, from WHO Director-General's opening remarks at the media briefing on COVID-19 - 11 March 2020: https://www.who.int/director-general/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---11-march-2020

Xu, S., Yung, M., & Wang, J. (2021, April 28). Seeking Foundations for the Science of Cyber Security: Editorial for Special Issue of Information Systems Frontiers. Information Systems Frontiers, 263-267.

Xulu, H. (2022). The New Private Security: Regulating Cybersecurity Services in South Africa. Private Security Industry Regulatory Authority©.

Yan, D. (2020). A Systems Thinking for Cybersecurity Modeling. arXiv.

Zachariadis, M., Scott, S., & Barrett, M. (2013). Methodological Implications of Critical Realism for Mixed-Methods Research. MIS Quarterly, 37, 855--879. Retrieved from http://www.jstor.org/stable/43826004

Zetter, K. (2015, 8). Hackers Finally Post Stolen Ashley Madison Data | WIRED. Hackers Finally Post Stolen Ashley Madison Data | WIRED. Wired. Retrieved from https://www.wired.com/2015/08/happened-hackers-posted-stolen-ashley-madison-data/

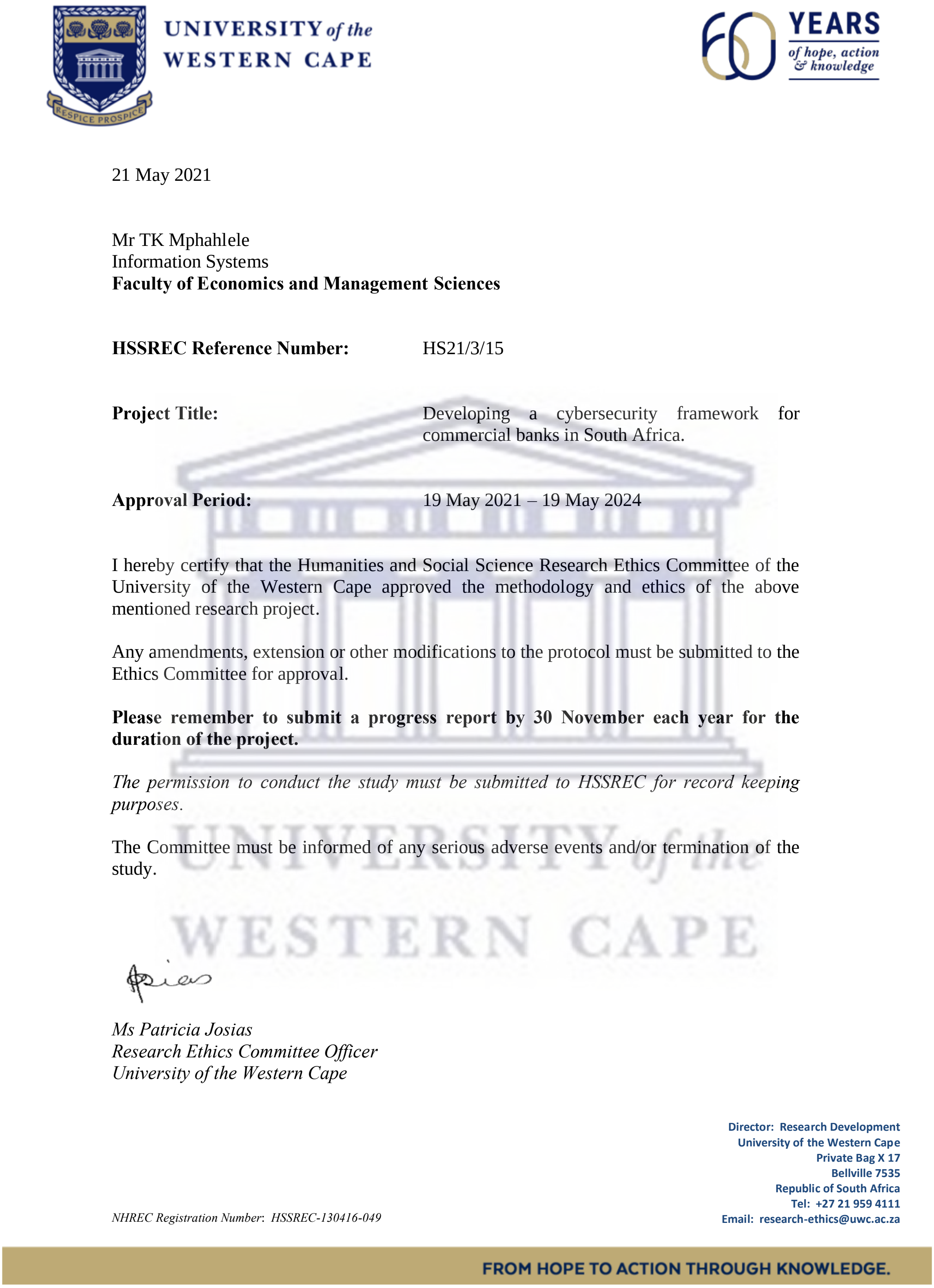
Zhang, Y., Xiao, Y., Ghaboosi, K., Zhang, J., & Deng, H. (2012). A survey of cyber crimes. Security and Communication Networks, 5, 422-437. doi:10.1002/sec.331

Zimmermann, V., & Renaud, K. (2019, November). Moving from a ‘human-as-problem” to a ‘human-as-solution” cybersecurity mindset. International Journal of Human-Computer Studies, 131, 169-187.

Zoto, E., Kianpour, M., Kowalski, S. J., & Lopez-Rojas, E. A. (2019, March). A Socio-technical Systems Approach to Design and Support Systems Thinking in Cybersecurity and Risk Management Education. Complex Systems Informatics and Modeling Quarterly (CSIMQ)(108), pp. 65-75.

Appendices

Appendix A – University Ethics Clearance



UNIVERSITY *of the* WESTERN CAPE

RESPICE PROSPICE

60 YEARS *of hope, action & knowledge*

21 May 2021

Mr TK Mphahlele
Information Systems
Faculty of Economics and Management Sciences

HSSREC Reference Number:	HS21/3/15
Project Title:	Developing a cybersecurity framework for commercial banks in South Africa.
Approval Period:	19 May 2021 – 19 May 2024

I hereby certify that the Humanities and Social Science Research Ethics Committee of the University of the Western Cape approved the methodology and 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.

The permission to conduct the study must 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 B – Research Project Information Sheet: Survey

Faculty of Economic and Management Sciences
Department of Information Systems

Research Project Information Sheet: Survey

Project Title:	**Developing a Cybersecurity Framework for Commercial Banks in South Africa**

What is this study about?

My name is Tlhologelo Mphahlele, and I am a student at the University of the Western Cape (South Africa) pursuing a Doctor of Philosophy (PhD) in Information Systems. I am conducting a study to identify the impediments commercial banks in South Africa face when developing cybersecurity frameworks. This study is solely for academic purposes. However, the results of this research may also be shared with commercial banks within South Africa and cybersecurity professionals.

What will I be asked to do if I agree to participate?

If you agree to participate in this research project, you will be asked to respond to several structured questions. This should take approximately 15 minutes. If you do not want to answer any questions, you do not have to.

Would my participation in this study be kept confidential?

You are not required to provide personal details, such as your name, address or identity number. Therefore, all other information, such as your age, education, employment status, etc., is anonymous.

What are the risks of this research?

There are no known risks associated with participating in this research process. This research will not expose you to any harm due to your participation.

What are the benefits of this research?

The outcome of this study will be used to develop a conceptual Cybersecurity Framework for Commercial Banks in South Africa. Secondly, the study will create awareness and guide cybersecurity practitioners within commercial banks in South Africa concerning cybersecurity culture, policies, and frameworks. Lastly, it will provide an industry best practice framework that information systems professionals can use and contribute knowledge to the Information Systems discipline.

Do I have to be in this research, and may I stop participating at any time?

Your participation in the survey is ultimately and entirely voluntary. You may choose not to take part at all. If you decide to participate in this survey, you may stop participating anytime.

What if I have questions?

If you have any questions, feel free to contact the study leader:

Contact details of project leader (study supervisor)

Name: Joel Chigada
University of the Western Cape, Department of Information Systems
Cell: +27745356824
Email: jchigada@uwc.ac.za

Contact details of the student

Name: Tlhologelo Mphahlele
Cell: +27796927438
Email: mphahleletk@gmail.com / 3342081@myuwc.ac.za

Contact details for the Humanities and social sciences research committee.

Research Development
Tel: +27 21 959 4111
Email: research-ethics@uwc.ac.za

University of the Western Cape

Faculty of Economic and Management Sciences

Department of Information Systems

Research Participant Consent Form: Survey

Project Title:	**Developing a Cybersecurity Framework for Commercial Banks in South Africa**

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 have had the opportunity to ask questions about the project.		
2. I understand that my participation is voluntary and that I can withdraw at any time without giving any reason or negative consequences.		
3. I understand that I am free to decline should I not wish to answer any particular question or questions.		
4. I understand that my responses and personal data will be kept strictly confidential. I give permission for the research team members to access 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 from the research.		
5. I agree that my data will be used in future research.		
6. I agree to take part in the above research project.		

_______________________ _____________ ____________________

Name of Participant Date Signature

(*Or legal representative*)

_______________________ _____________ ____________________

Name of person taking consent Date Signature

<u>Contact details of the study supervisor:</u>

Name: Joel Chigada

University of the Western Cape, Department of Information Systems

Cell: +27745356824

Email: jchigada@uwc.ac.za

<u>Contact details of the student</u>

Name: Tlhologelo Mphahlele

Cell: +27796927438

Email: mphahleletk@gmail.com / 3342081@myuwc.ac.za

Contact details for the Humanities and social sciences research committee.

Research Development

Tel: +27 21 959 4111

Email: research-ethics@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*

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 Survey

Project Title:	**Developing a Cybersecurity Framework for Commercial Banks in South Africa**

Researcher:

Tlhologelo Mphahlele

Email: mphahleletk@gmail.com / 3342081@myuwc.ac.za

Cell: +27 79 692 7438

Dear Respondent

My name is Tlhologelo Mphahlele; I am a PhD candidate in the Department of Information Systems, Faculty of Commerce at the University of the Western Cape. I am researching "Developing a Cybersecurity Framework for Commercial Banks in South Africa," so I invite you to participate in this study. Participation in this study is voluntary, and you can withdraw from the study at any time. Your responses will be treated in the strictest confidence, remain confidential and will be invaluable to completing this study. You will not be requested to supply identifiable or sensitive information in this research. The survey will take approximately 15 minutes to complete. By participating in this survey, you implicitly consent to participate in the research study. Please contact the researcher if you have any questions regarding the research.

SECTION A: DEMOGRAPHIC INFORMATION

In this section, you must mark your answer with an X.

Indicate your gender

Gender	
Male	
Female	
Prefer not to answer	

Indicate your age

18-25 years	
26-35 years	
36-45 years	
46-55 years	
56+ years	

Indicate your employer

Absa South Africa	
Standard Bank Group	
First National Bank South Africa	
Capitec Bank South Africa	
Nedbank South Africa	
African Bank South Africa	
Other (specify)	

What is your highest qualification?

National Diploma	
Bachelor’s Degree	
Honours	
Masters Degree	
Doctorate	
Other (specify)	

What is your current position/title?

Manager (specify)	
Information Systems Engineer	
Chief Information Security Officer	
Cybersecurity Specialist	
Fraud Specialist	
Risk Specialist	
Software Developer	
Other (specify)	

How many years of experience do you have?

Less than 1 year	
1-5 years	
6-10 years	
11-20 years	
More than 21 years +	

Indicate your race.

Black	
White	
Indian	
Coloured	
Asian	
Other (specify)	
Prefer not to answer	

SECTION B: CYBERSECURITY IMPEDIMENTS

In this section, you must select only one choice representing your viewpoint. Regarding cybersecurity within the commercial bank where you are employed where applicable. Please indicate your level of agreement with the following statements:

	Strongly Disagree	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**
I know how HB affects cybersecurity within the institution.	1	2	3	4	5
Does HB significantly affect cybersecurity within the institution?	1	2	3	4	5
Rules such as BYOD make it easier for the institution to protect its assets.	1	2	3	4	5
The development of an effective security framework is critical.	1	2	3	4	5
I know where to access the cybersecurity guidelines for the institution.	1	2	3	4	5
I follow all the rules and regulations outlined in the security guidelines.	1	2	3	4	5
I trust the cybersecurity protocols to identify, protect, detect, respond, and recover from cybersecurity threats.	1	2	3	4	5
I am prepared to circumvent the cybersecurity protocols in place to get my job done.	1	2	3	4	5
The institution has imposed some cybersecurity protocols that make it difficult for me to do my job.	1	2	3	4	5
I know my cybersecurity responsibility within the institution.	1	2	3	4	5
If a cybersecurity incident occurs, I know the steps needed to report and contain the incident.	1	2	3	4	5
The training offered by the institution helps me understand cybersecurity and how to protect myself and the institution.	1	2	3	4	5
I am aware of the impact cyber-attacks have on the institution.	1	2	3	4	5
I am aware of cybersecurity incidents that have happened at other commercial banks.	1	2	3	4	5
I am aware of the cybersecurity frameworks the institution has adopted.	1	2	3	4	5
I am aware of some cyber threats commercial banks face in South Africa.	1	2	3	4	5

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: Interview

Project Title:	**Developing a Cybersecurity Framework for Commercial Banks in South Africa**

What is this study about?

My name is Tlhologelo Mphahlele, and I am a student at the University of the Western Cape (South Africa) pursuing a Doctor of Philosophy (PhD) in Information Systems. I am conducting a study to identify the impendent commercial banks in South Africa face when developing cybersecurity frameworks. This study is solely for academic purposes. However, the results of this research may also be shared with commercial banks within South Africa and cybersecurity professionals.

What will I be asked to do if I agree to participate?

If you agree to participate in this research project, you will be asked to respond to several structured questions. This should take approximately 40 minutes. If you do not want to answer any questions, you do not have to.

Would my participation in this study be kept confidential?

You are not required to provide personal details, such as your name, address or identity number. Therefore, all other information, such as your age, education, employment status, etc., is anonymous.

What are the risks of this research?

There are no known risks associated with participating in this research process. This research will not expose you to any harm due to your participation.

What are the benefits of this research?

The outcome of this study will be used to develop a conceptual Cybersecurity Framework for Commercial Banks in South Africa. Secondly, the study will create awareness and guide cybersecurity practitioners within commercial banks in South Africa concerning cybersecurity culture, policies, and frameworks. Lastly, it will provide an industry best practice framework that information systems professionals can use and contribute knowledge to the Information Systems discipline.

Do I have to be in this research, and may I stop participating at any time?

Your participation in the survey is ultimately and entirely voluntary. You may choose not to take part at all. If you decide to participate in this survey, you may stop participating anytime.

What if I have questions?

If you have any questions, feel free to contact the study leader:

Contact details of project leader (study supervisor)
Name: Joel Chigada
University of the Western Cape, Department of Information Systems
Cell: +27745356824
Email: jchigada@uwc.ac.za

Contact details of the student
Name: Tlhologelo Mphahlele
Cell: +27796927438
Email: mphahleletk@gmail.com / 3342081@myuwc.ac.za

Contact details for the Humanities and social sciences research committee.
Research Development
Tel: +27 21 959 4111
Email: research-ethics@uwc.ac.za

Appendix C – Research Project Information Sheet: Interview

University of the Western Cape

Faculty of Economic and Management Sciences

Department of Information Systems

Research Participant Consent Form: Interviews

Project Title:	**Developing a Cybersecurity Framework for Commercial Banks in South Africa**

Please tick Yes or No to each of the following.

	Yes	**No**
7. I confirm that I have read and understand the information sheet explaining the above research project and have had the opportunity to ask questions about the project.		
8. I understand that my participation is voluntary and that I can withdraw at any time without giving any reason or negative consequences.		
9. I understand that I am free to decline should I not wish to answer any particular question.		
10. I understand that my responses and personal data will be kept strictly confidential. I give permission for the research team members to access 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 from the research.		
11. I agree that the interview may be recorded.		
12. I agree that my data will be used in future research.		
13. I agree to take part in the above research project.		

___________________________ ________________ ________________________

Name of Participant Date Signature

(*or legal representative*)

___________________________ _________________ ________________________

Name of person taking consent Date Signature

<u>Contact details of the study supervisor:</u>

Name: Joel Chigada
University of the Western Cape, Department of Information Systems
Cell: +27745356824
Email: jchigada@uwc.ac.za

Contact details of the student
Name: Tlhologelo Mphahlele
Cell: +27796927438
Email: mphahleletk@gmail.com / 3342081@myuwc.ac.za

Contact details for the Humanities and social sciences research committee.
Research Development
Tel: +27 21 959 4111
Email: research-ethics@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*

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 Interview

Project Title:	**Developing a Cybersecurity Framework for Commercial Banks in South Africa**

Researcher:

Tlhologelo Mphahlele

Email: mphahleletk@gmail.com / 3342081@myuwc.ac.za

Cell: +27 79 692 7438

Dear Participant

My name is Tlhologelo Mphahlele, and I am a PhD candidate in the Department of Information Systems, Faculty of Commerce at the University of the Western Cape. I am researching "Developing a Cybersecurity Framework for Commercial Banks in South Africa," so I invite you to participate in this study. Participation in this study is voluntary, and you can withdraw from the study at any time. Your responses will be treated in the strictest confidence, remain confidential and will be invaluable to completing this study. You will not be requested to supply identifiable or sensitive information in this research. The interview will take approximately 45 minutes. By participating in this interview, you implicitly consent to participate in the research study. Please contact the researcher if you have any questions regarding the research.

SECTION A: DEMOGRAPHIC INFORMATION

In this section, you must mark your answer with an X.

Indicate your gender

Gender	
Male	
Female	
Prefer not to answer	

Indicate your age

18-25 years	
26-35 years	
36-45 years	
46-55 years	
56+ years	

Indicate your employer

Absa South Africa	
Standard Bank Group South Africa	
First National Bank South Africa	
Capitec Bank South Africa	
Nedbank South Africa	
African Bank South Africa	
Other (specify)	

What is your highest qualification?

National Diploma	
Bachelor’s Degree	
Honours	
Master’s Degree	
Doctorate	
None	
Other (specify)	

What is your current position/title?

Manager (specify)	
Information Systems Engineer	
Chief Information Security Officer	
Cybersecurity Specialist	
Fraud Specialist	
Risk Specialist	
Software Developer	
Other (specify)	

How many years of experience do you have?

Less than 1 year	
1-5 years	
6-10 years	
11-20 years	
More than 21 years +	

Indicate your race

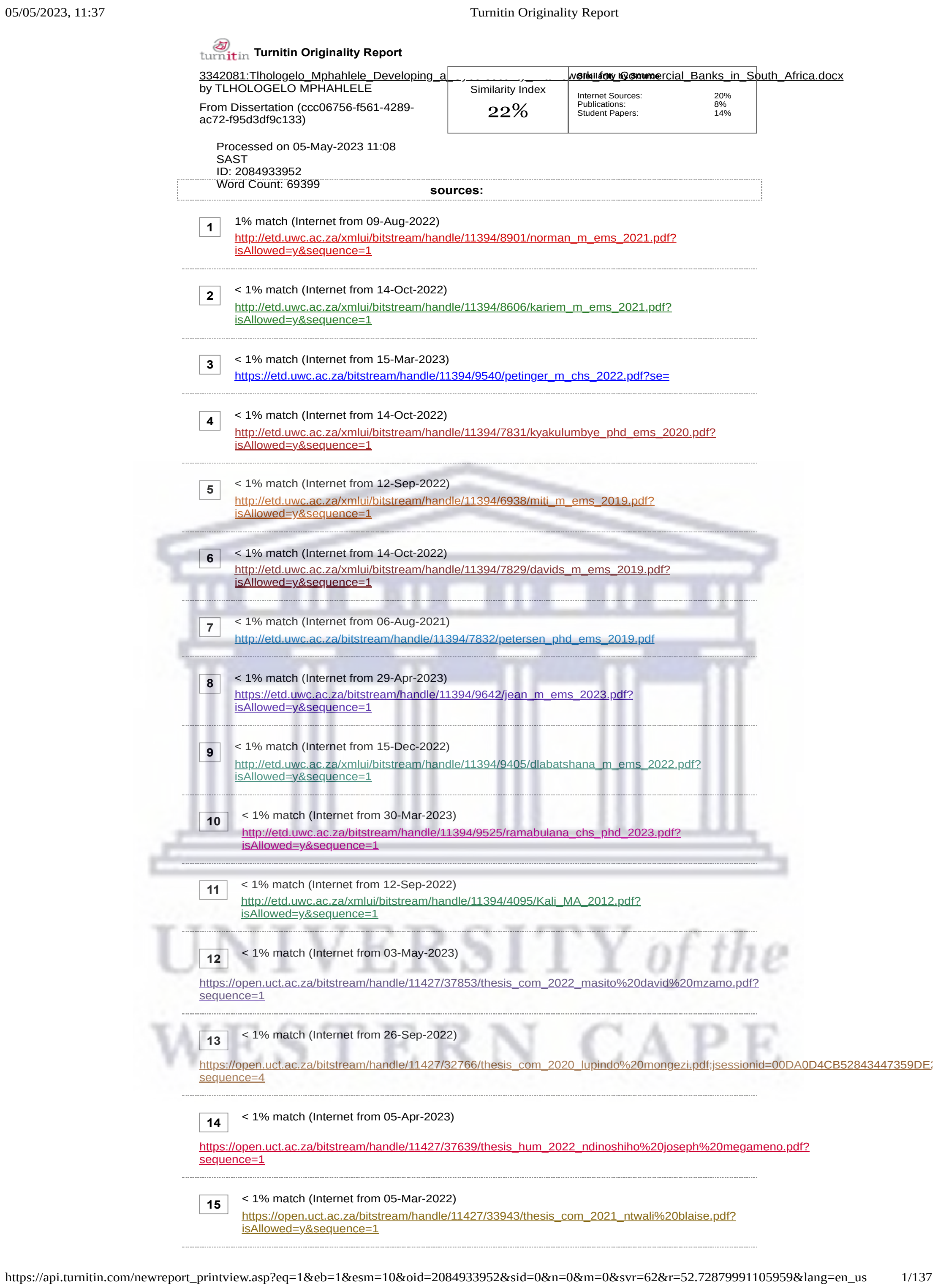
Black	
White	
Indian	
Coloured	
Asian	
Other (specify)	
Prefer not to answer	

SECTION B: CYBERSECURITY IMPEDIMENTS

In this section, you are requested to answer the questions honestly and based on your experiences and views.

1. What cybersecurity challenges are you aware of that banks face from an internal and external perspective?
2. Which cybersecurity frameworks are you aware of within your bank?
3. Do you know what benefits these frameworks offer and what they entail?
4. Do you think the adoption of the current cybersecurity frameworks is effective in protecting the institution? What factors impede your bank from developing an effective cybersecurity framework if not?
5. Why do you think banks continue to suffer from internal and external cybersecurity attacks and threats?
6. Which interventions do you know are in place to protect and mitigate the threats faced by the banks?
7. How do you think human behaviour contributes to developing cybersecurity frameworks in banks?
8. How do cyber-attacks and threats impact the operations of the bank?
9. Do you think cyber-attacks and threats are considered at every stage of a bank process?

Appendix D – Turnitin Report



05/05/2023, 11:37 Turnitin Originality Report

Turnitin Originality Report

3342081:Tlhologelo_Mphahlele_Developing_a[illegible]work_for_Commercial_Banks_in_South_Africa.docx
by TLHOLOGELO MPHAHLELE

From Dissertation (ccc06756-f561-4289-ac72-f95d3df9c133)

Processed on 05-May-2023 11:08
SAST
ID: 2084933952
Word Count: 69399

Similarity Index	Similarity by Source	
22%	Internet Sources:	20%
	Publications:	8%
	Student Papers:	14%

sources:

1 1% match (Internet from 09-Aug-2022)
http://etd.uwc.ac.za/xmlui/bitstream/handle/11394/8901/norman_m_ems_2021.pdf?isAllowed=y&sequence=1

2 < 1% match (Internet from 14-Oct-2022)
http://etd.uwc.ac.za/xmlui/bitstream/handle/11394/8606/kariem_m_ems_2021.pdf?isAllowed=y&sequence=1

3 < 1% match (Internet from 15-Mar-2023)
https://etd.uwc.ac.za/bitstream/handle/11394/9540/petinger_m_chs_2022.pdf?se=

4 < 1% match (Internet from 14-Oct-2022)
http://etd.uwc.ac.za/xmlui/bitstream/handle/11394/7831/kyakulumbye_phd_ems_2020.pdf?isAllowed=y&sequence=1

5 < 1% match (Internet from 12-Sep-2022)
http://etd.uwc.ac.za/xmlui/bitstream/handle/11394/6938/miti_m_ems_2019.pdf?isAllowed=y&sequence=1

6 < 1% match (Internet from 14-Oct-2022)
http://etd.uwc.ac.za/xmlui/bitstream/handle/11394/7829/davids_m_ems_2019.pdf?isAllowed=y&sequence=1

7 < 1% match (Internet from 06-Aug-2021)
http://etd.uwc.ac.za/bitstream/handle/11394/7832/petersen_phd_ems_2019.pdf

8 < 1% match (Internet from 29-Apr-2023)
https://etd.uwc.ac.za/bitstream/handle/11394/9642/jean_m_ems_2023.pdf?isAllowed=y&sequence=1

9 < 1% match (Internet from 15-Dec-2022)
http://etd.uwc.ac.za/xmlui/bitstream/handle/11394/9405/dlabatshana_m_ems_2022.pdf?isAllowed=y&sequence=1

10 < 1% match (Internet from 30-Mar-2023)
http://etd.uwc.ac.za/bitstream/handle/11394/9525/ramabulana_chs_phd_2023.pdf?isAllowed=y&sequence=1

11 < 1% match (Internet from 12-Sep-2022)
http://etd.uwc.ac.za/xmlui/bitstream/handle/11394/4095/Kali_MA_2012.pdf?isAllowed=y&sequence=1

12 < 1% match (Internet from 03-May-2023)
https://open.uct.ac.za/bitstream/handle/11427/37853/thesis_com_2022_masito%20david%20mzamo.pdf?sequence=1

13 < 1% match (Internet from 26-Sep-2022)
https://open.uct.ac.za/bitstream/handle/11427/32766/thesis_com_2020_lupindo%20mongezi.pdf;jsessionid=00DA0D4CB52843447359DE
sequence=4

14 < 1% match (Internet from 05-Apr-2023)
https://open.uct.ac.za/bitstream/handle/11427/37639/thesis_hum_2022_ndinoshiho%20joseph%20megameno.pdf?sequence=1

15 < 1% match (Internet from 05-Mar-2022)
https://open.uct.ac.za/bitstream/handle/11427/33943/thesis_com_2021_ntwali%20blaise.pdf?isAllowed=y&sequence=1

https://api.turnitin.com/newreport_printview.asp?eq=1&eb=1&esm=10&oid=2084933952&sid=0&n=0&m=0&svr=62&r=52.72879991105959&lang=en_us 1/137

A contributing factor to the similarity index generated by Turnitin was sections of the table of contents, acknowledgements, declaration, list of abbreviations and the appendix section with the data collection guides.