

https://dspace.org/

The perceived impact of Emerging Technologies on Cybersecurity in the South African financial sector

Philips, Denzil

2022
University of the Witwatersrand, Johannesburg
https://hdl.handle.net/10539/39909
Philips, Denzil. (2022). The perceived impact of Emerging Technologies on Cybersecurity in the South African financial sector [Master's dissertation, University of the Witwatersrand, Johannesburg]. WireDSpace.

Downloaded from a DSpace repository. https://dspace.org/

The perceived impact of Emerging Technologies on Cybersecurity in the South African financial sector

by

Denzil Phillips

2488813 (Research Report)

2488813@students.wits.ac.za / 0842001038

Supervisor: Dr Kiru Pillay

A research report submitted to the Faculty of Commerce, Law and Management, University of the Witwatersrand, in fulfillment of the requirements for the degree of Master of Management in the field of Digital Business

Johannesburg, 2022

DEDICATION

This research is dedicated to my wife and sons for their endless support throughout this research process.

DECLARATION

I, Denzil Phillips, declare that this research report is my own work apart from as indicated in the references and acknowledgments. This report is submitted as per the requirements in partial fulfillment for the degree of Master of Management in the field of Digital Business through the University of the Witwatersrand, Business School Johannesburg.



(Denzil Phillips)

22 Nantes Street, Suideroord, 2091
Signed at ……

29 **June**
On the …….. Day of …… 2023

ABSTRACT

This study is based on the investigation of what is the perceived impact of emerging technologies on cybersecurity in South African financial institutions. New and emerging technologies have made significant advancements in many industries that can be very disruptive in nature, and the majority of these technologies have changed the cyber threat landscape as well. These include, among other things, cloud computing, artificial intelligence, and machine learning. The study offers insight into how these emerging technologies affect the cybersecurity of financial institutions in South Africa.

The study consisted of Information technology risk and cybersecurity individuals. The sample size of 11 individuals was seen as sufficient based on the spread across the financial sector and the experience within the various industries. The individuals were from banks, insurers and market infrastructures within the South African financial sector.

The sample focused on key financial institutions specifically banks, insurers, and market infrastructures, based in different provinces in South Africa such as Johannesburg and Cape Town where the impact could be systemic in the country. A qualitative study was adopted by the researcher based on systems theory to determine the relationship between the adoption of emerging or new technologies and the impact it has on cybersecurity.

There were various responses from the different institutions, focusing on the adoption of emerging technologies, the effects of this adoption on the cybersecurity environment, the risk and vulnerability management processes, and the ability to adapt and respond to new cybersecurity risks introduced by emerging technologies.

The results of the study found that there is a clear link between the adoption of emerging technologies and the increase in cybersecurity requirements with emerging technologies significantly impacting the cybersecurity domain/function.

KEYWORDS

Artificial Intelligence, Cloud Computing, Cybersecurity, Digital Transformation, Financial Sector, Machine Learning, Quantum Computing.

TABLE OF CONTENTS

DEDICATION…… ii

DECLARATION…. iii

ABSTRACT…… iv

KEYWORDS…… v

LIST OF ACRONYMS x

LIST OF FIGURES xi

LIST OF TABLES…… xii

CHAPTER 1. INTRODUCTION 13

1.1 BACKGROUND OF THE STUDY 13
1.2 PROBLEM STATEMENT 14
1.3 MAIN RESEARCH PURPOSE 16
1.4 RESEARCH OBJECTIVES 17
1.4.1 MAIN OBJECTIVE 17
1.5 RATIONALE 17
1.6 DELIMITATIONS OF THE STUDY 18
1.7 DEFINITION OF TERMS 18
1.8 ASSUMPTIONS 19
1.9 CHAPTER OUTLINE 19
1.9.1 INTRODUCTION 19
1.9.2 LITERATURE REVIEW 19
1.9.3 RESEARCH METHODOLOGY 19
1.9.4 PRESENTATION OF RESULTS 19
1.9.5 INTERPRETATION OF RESULTS 20
1.9.6 CONCLUSION AND RECOMMENDATIONS 20
1.10 CONCLUSION 20

CHAPTER 2. LITERATURE REVIEW 21

2.1 INTRODUCTION 21
2.2 CONCEPTUAL UNDERSTANDING OF THE KEY TERMS 22
2.2.1 EMERGING TECHNOLOGIES AND DIGITAL TRANSFORMATION 22

2.2.2 Cybersecurity 24
2.2.3 The rise of the cyber threat and the need for effective cybersecurity controls 25
2.2.4 Financial Sector 25
2.3 Research Questions 26
2.3.1 Primary Research Question 26
2.3.2 Sub-Question 26
2.3.3 Proposition 26
2.4 Prior studies of Emerging Technologies and Cybersecurity 26
2.4.1 The adoption of emerging technologies 26
2.4.2 The significance of cybersecurity 27
2.5 The impact of emerging technologies on cybersecurity 28
2.5.1 Overview 28
2.5.2 The adverse relationship between Emerging Technologies and Cybersecurity 29
2.5.3 The overall Impact of Emerging Technologies on Cybersecurity 30
2.6 The South African context 34
2.7 Theoretical Framework 35
2.7.1 Systems Theory 37
2.7.2 Conclusion of Theoretical Framework 38
2.8 Conclusion of Literature Review 39

CHAPTER 3. RESEARCH METHODOLOGY 41

3.1 Research approach 41
3.2 Research design 41
3.3 Data collection methods 42
3.4 Population and sample 42
3.4.1 Population 42
3.4.2 Sample and sampling method 42
3.5 The research instrument 43
3.6 Procedure for data collection 44
3.7 Data analysis strategies and interpretation 45
3.8 Possible limitations and challenges of the Study 45
3.9 Quality Assurance 45
3.9.1 Dependability 45
3.9.2 Credibility 46
3.9.3 Transferability 46
3.10 Ethical considerations 46
3.11 Proposed schedule and timelines 46

CHAPTER 4. PRESENTATION OF RESULTS 47

4.1 INTRODUCTION 47
4.2 PROFILE OF RESPONDENTS 47
4.2.1 POSITION AND SECTOR 47
4.3 QUALITATIVE RESULTS 48
4.4 THEMATIC ANALYSIS 49
4.4.1 CODING 50
4.4.2 EMERGING CODES AND THEMES 53
4.4.3 DEFINING THE THEMES 54
4.4.4 INTERVIEW RESULTS 55
4.5. RESULTS SUMMARY 64

CHAPTER 5. INTERPRETATION OF RESULTS 65

5.1 INTRODUCTION 65
5.2 THEME 1: EMERGING TECHNOLOGIES AND ITS ADOPTION 65
5.2.1 SUB-THEME: DIGITAL TRANSFORMATION STRATEGIES 67
5.3 THEME 2: CYBERSECURITY POSTURE AND CONTROLS 69
5.3.1 SUB-THEME: CYBERSECURITY RISK AND VULNERABILITY MANAGEMENT 71
5.4 THEME 3: IMPACT OF EMERGING TECHNOLOGIES ON CYBERSECURITY 72
5.4.1 SUB-THEME: ABILITY TO ADAPT AND RESPOND 74
5.5 SUMMARY OF ANALYSIS 75

CHAPTER 6. CONCLUSION AND RECOMMENDATIONS 76

6.1 INTRODUCTION 76
6.2 CONCLUSION OF THE RESEARCH STUDY 77
6.3 SUMMARY OF FINDINGS 78
6.3.1 EMERGING TECHNOLOGIES AND THEIR ADOPTION LIMITATIONS 78
6.3.2 CYBERSECURITY POSTURE AND CONTROLS 79
6.3.3 IMPACT OF EMERGING TECHNOLOGIES ON CYBERSECURITY 79
6.4 LIMITATIONS 80
6.5 RECOMMENDATIONS 80
6.6 SUGGESTIONS FOR FURTHER RESEARCH 81

REFERENCES 82

APPENDIX A 98

INTERVIEW QUESTIONNAIRE (ONLINE INTERVIEWS) 98

APPENDIX B……..... 100

PARTICIPANT INFORMATION SHEET 100

Annexure C……..... 102

CONSENT FORM..... 102

Annexure D……..... 104

ETHICAL CLEARANCE 104

Annexure E……..... 105

APPROVED TOPIC 105

Annexure F…… 106

CHECKLIST 106

Annexure G…… 107

TURNITIN..... 107

LIST OF ACRONYMS

AI	Artificial Intelligence
APT	Advanced Persistent Threat
AR	Augmented Reality
DoS	Denial of Service
DDoS	Distributed Denial of Service
DLP	Data Loss Prevention
IoT	Internet of Things
ML	Machine Learning
RPA	Robotics Process Automation
SOC	Security Operations Centre
TTP	Tactics, Techniques and Procedures
VR	Virtual Reality

LIST OF FIGURES

FIGURE 1 EMERGING TECHNOLOGY FOSTERS INCREASED CYBERSECURITY 14
FIGURE 2 NEW / EMERGING TECHNOLOGIES 16
FIGURE 3 THEMATIC ANALYSIS FOR RESEARCH STUDY 50

LIST OF TABLES

TABLE 1 DEFINITIONS OF TERMS 18
TABLE 2 PARTICIPANTS.....47
TABLE 3 DEDUCTIVE CODES…… 50
TABLE 4 INDUCTIVE CODES….....50
TABLE 5 EMERGING CODES AND THEMES…. 53

CHAPTER 1. INTRODUCTION

1.1 Background of the study

The journey towards digital transformation is underpinned by various types of emerging or new technologies such as cloud technologies, AI and ML, amongst others. The South African financial sector is undergoing significant technological change, with many institutions focused on digital transformation and creating digital strategies for the future (Radanliev et al., 2020). Emerging technologies are disrupting established financial services with fintechs also enjoying tremendous development in South Africa's financial industry. Payment services are increasingly going cashless, and using biometrics to make payments has also become more popular (Mittal, 2019). Digital transformation is a huge part of emerging technologies and has played a major role in the introduction of emerging technologies. According to Lee (2017), technologies such as artificial intelligence, machine learning, IoT and cloud technologies are recognised as major emerging technologies influencing technological development, regardless of the organisation adopting it. This, heightened by the availability of high-speed internet access, is creating a platform for disruption, and also increasing the cybersecurity risk (Deloitte, 2018). Chatfield & Reddick (2019) argue that the advent of IoT and the move to the cloud, for example, have greatly enhanced interconnected ecosystems, that is creating a larger spectrum of connectivity and increasing the need for greater cybersecurity based on the rise of cyber-attacks. In research conducted by Deloitte (2020), these technologies have also enhanced the financial ecosystem, although, also influencing the cybersecurity posture of the financial sector. This is highlighted by the increase in cyber incidents which continues to grow in both complexity and severity and is a function of an increasingly open and interconnected financial ecosystem. The advent of emerging technologies is increasing the cyber threat landscape (European Systemic Risk Board (ESRB), 2020). According to research from Pancholi and Strobl (2019), organisations rely on technologies and regardless of their digital footprint, are vulnerable to cyber breaches or incidents (Pancholi & Strobl, 2019). Emerging technologies disrupt the environment,

requiring additional focus on cybersecurity as depicted in Figure 1 below. One leads to an increase in the other.

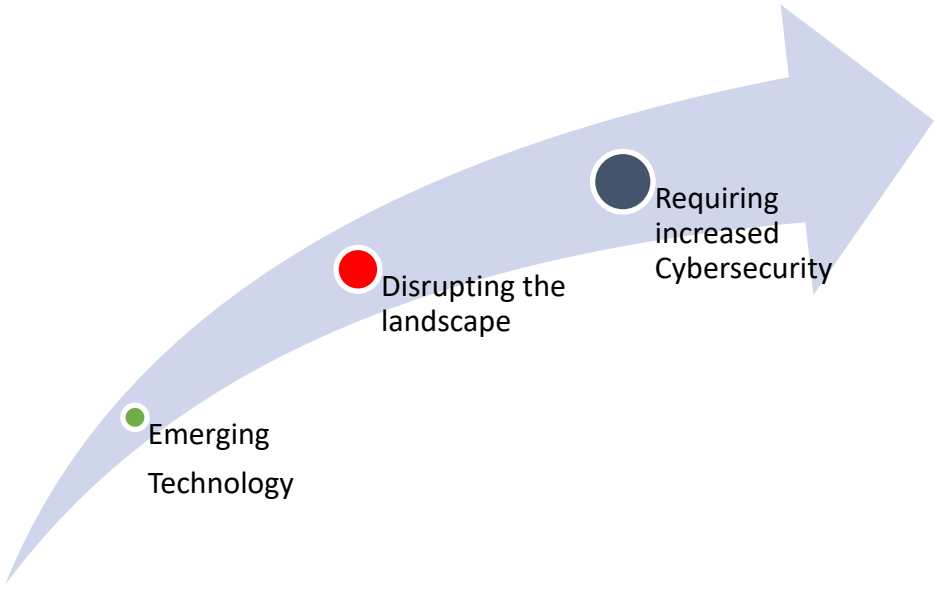


Figure 1: Emerging technology fosters increased cybersecurity (Chatfield & Reddick, 2019).

Emerging technologies are being explored by the financial sector, and being implemented at a rapid pace, disrupting the landscape, and exposing financial institutions to more cyber-attacks. Research undertaken by the World Economic Forum (WEF) (2022) highlights the rise of cyber incidents and the associated financial impacts, which have the potential to destabilise the financial services sector. It has been seen that disruptive emerging technologies are leading to additional benefits for the financial sector; however, it is also leading to adverse impact on the cybersecurity posture of these organisations (Deloitte, 2018).

1.2 Problem Statement

There are regular reports of the increased adoption of emerging or new technologies as well as the breakdown of cybersecurity controls of financial institutions or the increase in the cyber threat against the financial sector in many jurisdictions (Byrne, 2021). There are, however, fewer reports on the impact of one on the other from a South African perspective or if there is a clear relationship between the two factors (Wilkinson, 2011). The financial sector is a critical component of any country; the growth and survival of these organisations are important for the growth and

sustainability of the economy. The adoption of emerging technologies plays a major role in ensuring the growth and survival of these organisations, however, also introduces the risk of cyber threats. McKenna (2021) highlights that a major factor for organisations with the adoption of emerging technologies is an adequate and effective cyber control environment, and prioritising cybersecurity for the successful implementation of these emerging technologies is key. Furthermore, understanding this impact allows for greater synergy between the adoption or implementation of emerging technologies and the implementation of adequate controls. The lack of understanding of the impact of new or emerging technologies on the cybersecurity posture of financial institutions from an overall sector perspective places financial institutions at risk of new unknown cyber-attacks (Byrne, 2021).

This study tries to interrogate the perceived impact of the adoption or implementation of emerging technologies on the cybersecurity posture of financial institutions in South Africa and determine if there is a relationship or influence of one on the other. Figure 2 below highlights the synergy that's required between new/emerging technologies and cybersecurity in the financial sector.

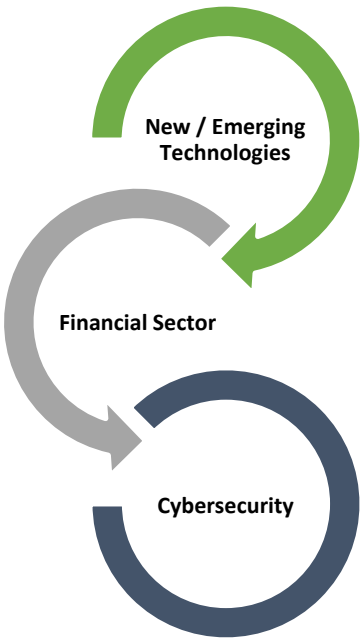


Figure 2: New / emerging Technologies require institutions to relook at their cybersecurity (Wu et al., 2018).

1.3 Main Research Purpose

The advancement in technology is ongoing and so is the continuing rise in cyber threats, each having impact on the other. The study explores the perceived impact of emerging technologies on the cybersecurity posture of South African financial sector organisations. The adoption of emerging technologies is often linked to digital transformation initiatives and impacts the cybersecurity domain of organisations.

Emerging technologies are being widely explored and financial institutions are actively adopting these technologies; from the drive towards increasing the mobile footprint to the reduction of face-to-face interaction, or even branch closures as a result of other effects like COVID-19, thus increasing transactions or other activities across the internet (Higgs et al., 2022). Thus, resulting in a larger landscape for cyber threats. The increased landscape together with the unknowns introduced as a result of the adoption of emerging technologies creates uncertainty for financial institutions in the cyber realm with existing cybersecurity measures not adequately tested against these unknowns (Wu et al., 2018).

The focus of this research is to interrogate the perceived impact of emerging technologies on the cybersecurity posture of financial institutions in South Africa. The analysis will be looking at what's perceived from an individual financial institution perspective while also attempting to reach that point of saturation from the data obtained from the semi-structured interviews where what is perceived from the results at an individual level is the same as that perceived across the financial sector and country as a whole. The review tries to cross-examine the level of impact that emerging technologies have on cybersecurity. If there is a clear relationship between the adoption of emerging technologies and the impact on cybersecurity according to systems theory. The key problem is highlighted where there is limited literature to determine the impact from a South African perspective. Moreover, the additional context required to understand how emerging technologies influence cybersecurity in the South African financial sector is also not evident.

1.4 Research objectives

1.4.1 *Main Objective*

Investigate the impact of emerging technologies on the cybersecurity posture in the South African financial sector

Understand the changes in the cybersecurity domain due to the adoption of emerging technologies in the South African financial sector.

1.5 Rationale

The study was aimed at determining the impact of emerging technologies on the cybersecurity posture of financial institutions in South Africa. This was based on preliminary information that highlighted that although the impact was ubiquitous, the literature available captures this internationally, but not necessarily from a South African perspective. The limited literature makes it problematic to validate what is already known. The literature review helped to identify the missing information in the current studies. Systems theory is adopted to determine if there is a relationship between the adoption of emerging technologies and the impact on cybersecurity. According to Wilkinson (2011), systems theory is based on the premise that it is better to understand a system's individual pieces in the context of how they interact with one another and with other systems as a whole (Wilkinson, 2011). Systems theory is built on the evidence that the effect of a factor is influenced by another factor, or the factors work together to create a result (Arnold, 2013).

This study provides an understanding of the impact of emerging technologies on the cybersecurity domain in South African financial institutions. While there is existing research on the increased adoption of emerging technologies, the increasing risk of cyber threats, and on the increased requirements for cybersecurity, there is limited research available on these impacts from a South African perspective. The study investigates the impact of the adoption of new technologies on the cybersecurity domain.

1.6 Delimitations of the Study

The review, although holistically looking at digital transformation is limited to the most common emerging technologies adopted such as AI, ML and cloud computing.

The study focuses on the South African financial sector and was exclusively undertaken with banks, insurers and market infrastructures.

1.7 Definition of terms

Cyber attack	Attempts to obtain access to private or personal information in an attempt to change, delete, modify, etc. the information, attempts to disrupt business operations, extort money, etc. (Mishra, 2023).
Cybercrime	Includes aspects such as malware, fraud and Identity theft (Mishra, 2023).
Cybersecurity	The defence of the information and/or information systems availability, confidentiality, and integrity (Glossary, n.d. 2022).
Cybersecurity posture	refers to an institution's overall cybersecurity control environment, and how it can identify, protect, detect, respond and recover from cyber-attacks (Rosencrance, 2022).
Cyber threats	The probability of a cyber-attack occurring. (Mishra, 2023).
Digital Transformation	Organisational change through the use of new or emerging digital technologies (BCG Global, 2022).
Emerging Technologies	Radical, fast-growing, new technologies or the development of existing technologies (Stăncioiu, 2017).
Financial Sector	The financial services segment of the economy consisting of various organisations including banks, insurers, investment houses, market infrastructures, etc. (Hougaard, 2022).

Table 1 Definitions

1.8 Assumptions

The assumption was that the data for the study was obtained from semi-structured interviews conducted with banking, insurance and market infrastructure personnel, with knowledge in the respective fields, obtaining a holistic view from a financial perspective and not focusing on broader industries. It is, however, assumed that the technology would similarly affect any industry, having the same impact on cyber security. It's further assumed that many emerging technologies are introduced during organisations' digital journeys and are a major part of digital transformation. It's assumed that the individuals interviewed were factual in their responses.

1.9 Chapter Outline

1.9.1 *Introduction*

Chapter one highlights the background, research problem, research objective, rationale, limitations, significance, definitions, assumptions, and chapter outline.

1.9.2 *Literature Review*

Chapter two provides definitions of key terms including, Cybersecurity, Digital Transformation, and Emerging Technologies, and the literature review together with the objective of the literature review.

1.9.3 *Research Methodology*

Chapter three outlines the research approach, design, data collection, population, sampling, data analysis strategies, possible limitations of the study and quality assurance.

1.9.4 *Presentation of Results*

Chapter four provides a view of the data collected from the semi-structured interviews outlining the data that came of the interviews. The data were linked to various codes and overall themes which are highlighted in the chapter.

1.9.5 *Interpretation of Results*

Chapter five provides a view of the analysis of the data and highlights the results of the topic i.e., whether there is a perceived impact of emerging technologies on cyber security and any additional insights that came out of the data.

1.9.6 *Conclusion and recommendations*

Chapter six concludes the research report, highlights if there is a link to systems theory and further highlights some of the recommendations.

1.10 Conclusion

The introduction of the report highlights the increase in emerging technologies as well as the rise of the cyber threat, with both existing in the same realm. The effective growth of organisations specifically in the financial sector that's directly impacted by the adoption of emerging technologies. Organisations face the risk of falling behind the curve if these technologies are not adopted, but also face additional risk exposures if they do. Emerging technologies have evolved to become key in the way organisations have changed. This evolution has impacted the cybersecurity environment both positively and negatively with technologies such as AI, ML, Cloud Computing, etc. used for both malicious cyber activities as well as to protect organisations' systems against these cyber-attacks (Sharma, 2021). Furthermore, this adoption has an impact on the cybersecurity posture of financial institutions; the impact is perceived disparately based on the technologies adopted. The South African financial sector as a whole and down to each institution has been impacted by technological change but has embraced the technological changes over time; the bigger financial institution has also constantly tested their readiness against various cyber threats (Medoh & Telukdarie, 2022). The challenges arise with the vast quick changes in technologies that increase the cyber risk and the institutions' ability to adapt and respond adequately and effectively (Gcaza & von Solms, 2017).

CHAPTER 2. LITERATURE REVIEW

2.1 Introduction

The key objective of the literature review was to assess the data in the available literature, both from present or prior studies on the adoption of emerging technologies and the impact these emerging technologies have on cybersecurity or the overall cybersecurity posture of financial institutions in the South African financial sector. The chapter focuses on emerging technologies with digital transformation as a sub-category of emerging technologies and the relationship it has with cybersecurity or the impact that emerging technologies have on cybersecurity requirements in financial institutions.

Cybersecurity continues to grow, with threat actors always looking at vulnerabilities to exploit in organisations; often heightened by the introduction of new technologies as these new technologies are sometimes implemented with limited controls at the onset. Robust cybersecurity protocols are essential for protecting organisations from cyberattacks and data breaches, as well as for preserving online privacy and trust.

The review contains key aspects of technology that are pivotal to this study. The first path of the literature review is focused on key high-level definitions; the second part of the review is focused on prior studies, trying to ascertain what was previously ubiquitously known or discovered and the South African context; the third part of the review is focused on the theoretical framework, linked to systems theory and trying to determine if there is a relationship between emerging technologies and cybersecurity and to address how emerging technologies can enhance or hinder cybersecurity, as well as the implications thereof; and the final part of the review will be focused on the conclusion of the literature review.

2.2 Conceptual understanding of the key terms

2.2.1 Emerging Technologies and Digital Transformation

Emerging technologies are changing the technological landscape and can be defined as new technology trends, or technology trends with signs of creating new opportunities or a competitive edge and include technologies such as artificial intelligence (AI), machine learning (ML), cloud computing and the Internet of Things (IoT) (Chatfield & Reddick, 2019).

Recent studies have highlighted that many organisations are driving towards technological change with competition being introduced through the adoption or implementation of emerging technologies such as Artificial Intelligence (AI), Machine Learning (ML), and cloud computing leading to an increase in technological transformation, including digital transformation (Vial, 2019). According to research by Gong and Ribiere (2021), there is a diverse range of definitions of digital transformation, its widely determined that a unified definition for any topic is required to improve the theory and application (Stock & Boyer, 2009). Gong and Ribiere (2021) presented their definition and highlighted that digital transformation includes massive change which is introduced by the introduction of new emerging and pioneering technologies that has the probability of greatly influencing the growth of the business and creating additional value for customers. A key driver as part of the digital transformation journey for organisations has also been defined as the adoption of emerging technologies and recognising of new growth potential to digitally transform the organisation through technology (Pereira et al., 2022). Digital transformation includes a plethora of digital technologies with many of these technologies known as emerging technologies (BCG Global, 2022). Organisations are required to strategically identify future growth opportunities, and understand the current technology landscape, however, looking at future technological advancements to take the organisation forward; looking at emerging technologies and the benefits associated with them (CompTIA, 2022).

The adoption of emerging technologies is important for the continued growth of organisations especially within the financial sector, as competitors are entering the

market with massive technological capabilities that are strongly impacting traditional financial institutions (Forbes, 2019). Many organisations have defined emerging technologies as a new trend with the opportunity to create niche markets or competitive edge. Technologies such as AI, as well as technological capabilities enhanced through the use of technologies such as ML, or even the migration to cloud technologies, are creating alternative operating models and increased potential for competitive advantage (Chatfield & Reddick, 2019). This, however, can be disruptive or create an element of surprise forced upon organisations. Therefore, organisations need to have the ability to respond to technological advances that can disrupt their standard operating models by exploiting the opportunities that emerging technologies introduce. Many Big Tech firms like Microsoft, Apple, Amazon Web Services, Google, etc. have entered the financial sector with the ability to offer financial products seamlessly without the difficulties experienced by traditional financial institutions, due to their ability to quickly adapt to emerging technologies (Forbes, 2019). Many organisations have failed to successfully exploit the advantages of emerging technologies and have faulted like Kodak, an organisation that was not able to respond to the emergence of digital and exploit the technology advancements which resulted in a major loss of market share. (Lucas & Goh, 2009b).

Emerging technologies have been proven to hugely affect organisations, whether it's the environment, the people or even the processes, extending to aspects such as people's way of life, the overall economy, and so much more. This often disrupts existing strategies and processes, requiring change; not entirely negative as positive aspects also emerge in terms of creating new opportunities. The effects could have larger ubiquitous impacts on the sector or country as a whole as it could drive potential economic growth, job opportunities, different industries and so on (Rodrigues et al., 2022b). Technologies like AI, ML, and Cloud computing have the potential to revolutionise the financial sector, increasing productivity and efficiency; creating different products and service offerings; developing better ways of processing e.g., payments and settlements, cross-border transactions, monitoring of foreign transactions, etc., however, also raising important ethical and social questions such as job displacement through AI-led technologies and the ethical implications of autonomous decision-making systems (Hatzivasilis et al., 2020).

Digital Transformation and Emerging technologies have often been used synonymously. In research from Lyu and Liu (2021), numerous new digital technologies are producing significant economic benefits across a range of industries thanks to the drive toward digital transformation. The most commonly used developing digital technologies are AI, Big Data, IoT, Cloud computing, etc. (Lyu & Liu, 2021).

2.2.2 Cybersecurity

The practice of deploying people, policies, processes, and technologies to safeguard organisations, their core systems, proprietary data, information assets, etc. from cyber threats is known as cybersecurity or the resultant cybersecurity posture of the organisation (Rosencrance, 2022). This can be related to ensuring that the organisation's processes and networks are secured by design (Gartner, 2022). This can include mechanisms such as identity and access management, system incident or event monitoring, and data loss prevention solutions that include various safeguards such as firewalls, endpoint protection, antivirus software, and monitoring tools, amongst others to secure the environment (CrowdStrike, 2022).

Cybersecurity has a larger ubiquitous impact on various sectors and society at large, because of the interconnectedness. Similarly, as emerging technologies like AI, ML and cloud computing become more prevalent, cybersecurity becomes even more critical and ensuring the maturing of the cybersecurity control environment is key to preventing malicious exploitation, system breaches, and data loss. etc. (Chatfield & Reddick, 2019). Strong cybersecurity practices help safeguard, organisations from data breaches and cyber-attacks which is also crucial for maintaining privacy and trust in online activities. With the increasing digitisation of personal information and online transactions, individuals need to trust that their data is adequately protected. Ensuring an effective control environment is pivotal to safeguarding enterprises from cyberattacks and data breaches. A lack of cybersecurity measures can erode trust and limit the adoption of digital technologies and services (Pancholi & Strobl, 2020).

Cybersecurity is influenced by emerging technologies that are becoming more accessible; and while these advancements allow for a paradigm change for these organisations, it also increases the cybersecurity risk exposure (Wu et al., 2018). The adoption of these technologies which leads to a paradigm shift in an organisation is

the key aspect of digital transformation. This, however, could have both beneficial and detrimental consequences for a company; where depending on the technology used, if implemented poorly with inadequate or ineffective controls, will introduce a variety of risks, including increased cybersecurity risk exposure. It is important to continuously improve cybersecurity practices simultaneously with the adoption of emerging technologies and remain vigilant against evolving threats to mitigate these impacts effectively which is enhanced by the more aggressive adoption of emerging technologies (Medoh & Telukdarie, 2022).

2.2.3 The rise of the cyber threat and the need for effective cybersecurity controls

Cyber threats continue to grow regardless of the industry and are often a result of an increasingly open and interconnected world. The growth of these threats are seen to be complex with the threat actors who are the malicious users often using disparate attack vectors which is the mode of attack (Sharma, 2021). Both the attack surface and the threat landscape is dynamic with threat actors always trying to attack; With the introduction of new and developing technologies like AI, ML, and the expansion of cloud technologies, additional threat vectors are often also introduced (Ukwandu et al., 2021).

2.2.4 Financial Sector

According to Hougaard (2022), the financial sector is the portion of the economy consisting of various organisations including banks and insurers, amongst others. The financial sector is a major part of the country's economy and according to research conducted by Varga et al. (2021), the financial sector is influenced by the growth in technology, with emerging technologies creating ongoing competition in the financial sector. The financial sector is also exposed to major regulatory requirements that assist in the financial stability of any economy. Financial stability within the financial sector helps to create opportunities, and with the advent of emerging technologies, the growth has been exponential, although the growth of cybercrimes has also dramatically increased, requiring organisations to have a robust cybersecurity posture (World Bank, 2022).

2.3 Research Questions

2.3.1 Primary Research Question

What is the impact of emerging technologies on the cybersecurity domain of financial institutions in South Africa?

2.3.2 Sub-Question

Is there a clear relationship between emerging technologies and cybersecurity?

2.3.3 Proposition

An increase in the adoption of emerging technologies causes and impact on the cybersecurity of financial institutions in South Africa.

2.4 Prior studies of Emerging Technologies and Cybersecurity

2.4.1 The adoption of emerging technologies

The world of technology is said to be evolving, a move towards a more digital ecosystem. A phrase by Klaus Schab and cited by Xu et al (2018) perfectly outlines this change, “We stand on the brink of a technological revolution that will fundamentally alter the way we live, work, and relate to one another. In its scale, scope, and complexity, the disruption will be unlike anything humankind has experienced before. We do not yet know just how it will unfold, but one thing is clear: the response to it must be integrated and comprehensive, involving all stakeholders of the global polity, from the public and private sectors to academic and civil society” (Xu et al., 2018). This creates a change to the standard operating practices of technology and the link between the physical and virtual environments in the cyber realm. According to research by Stăncioiu (2017), these emerging technologies have the potential to result in a dramatic alteration of the financial system or production process of the financial sector. The adoption of emerging technologies such as cloud computing AI, ML, virtual (VR) or augmented reality (AR), and IoT, amongst others

has allowed organisations to digitally transform, creating more efficiency and optimisation in organisations (Stăncioiu, 2017). Based on the research conducted by Stăncioiu (2017), additional disruption is seen where technologies like Robotics Process Automation (RPA) are being adopted to replace certain admin-intensive tasks in financial institutions and Robots are also being developed with the ability to do what was previously only possible for humans to do, reducing the need for certain workers.

Emerging technologies are strategically adopted by organisations to achieve their strategic objectives. Many organisations that may not be technology or digitally savvy organisations adopt digital technologies or digitally transform the organisation to try to obtain a competitive advantage (Guggenmos et al., 2022). According to a report by the WEF (2022), emerging technologies are a major factor or huge driver for technological disruption and prioritising this disruption is a key element to digitally transform. The drive of the phenomenon is noted throughout the world and is not necessarily linked to any particular continent, country, or organisation. The adoption of emerging technologies such as AI, ML and cloud computing, amongst others can lead to exponential growth of financial institutions, however, it can also lead to major disruptions of the financial system (PWC, 2021).

2.4.2 The significance of cybersecurity

Cybersecurity is the protection of information or data and information systems from damage, misuse, unauthorised access or modification, etc. (Glossary, n.d. 2022). According to NIST (2021), “A cybersecurity breach is an incident where the confidentiality, integrity, or availability of an information system is compromised”. Ransomware, unauthorised access to information systems, malware attacks, etc. are some examples of cybersecurity breaches (NIST, 2021).

Cyber-attacks or breaches give rise to increased investment in cybersecurity and also drive the strategic decisions of the organisation. The continued existence of organisations has become increasingly reliant on effective cybersecurity (Fernandez De Arroyabe et al., 2023). This is further influenced by the rise in the adoption of new or emerging technologies as existing cybersecurity measures may not be effective against new threats introduced based on these technologies (Karjalainen et al., 2019). In research by Fernandez De Arroyabe et al. (2023), they highlight that it’s imperative

that cybersecurity investment is a key strategic decision of organisations influenced by both the internal requirements of the organisation as well as the external environment, being the cyber threat landscape. This is further influenced by the existing capabilities and cyber threats or breaches as well as new threats introduced. The cost of cybersecurity mitigating controls against cyber breaches has dramatically increased over the years, negatively affecting many organisations, and making the correct investment key for cyber security. According to Shao et al. (2020), investment in cybersecurity is different for each organisation and although it's important to learn from other institutions with regards to cybersecurity, organisations should determine what's fit for purpose (Shao et al., 2020).

Cybersecurity in a sense does not provide any economic benefits or increased revenue, however, it is mechanisms that can prevent loss or something from happening, for example, a cyber breach leading to losses (Shao et al., 2020).

2.5 The impact of emerging technologies on cybersecurity

2.5.1 *Overview*

The cyber threat continues to grow; and can take many disparate structures and forms, exploiting vulnerabilities in people, processes, and technologies, leading to loss of sensitive data, unavailability of systems, changes to systems, etc. According to research by Caldwell (2011), massive increases in organisations exposed to data breaches as well as system outages were noted, with the constructs of technologies being key to these threats with emerging technologies heightening the exposure (Caldwell, 2011). As technologies advance, so do the cybersecurity requirements with the need for constant adaptability, highlighting the relationship between the two (Byrne, 2021). The landscape is continually changing with financial institutions adopting technologies such as AI, ML and cloud computing which in turn is increasing the nature and scale of the cyber ecosystem and providing a platform for exponential growth in cyber-attacks (Corallo et al., 2020). This accelerating pace of technological change is increasing the cybersecurity risk exposure requiring organisations to rapidly adapt their cybersecurity measures (Gartner, 2022).

2.5.2 *The adverse relationship between Emerging Technologies and Cybersecurity*

According to the OECD (2021), the introduction of AI-powered technology heightens cyber risk exposure and despite the many benefits, organisations have to be cautious and monitor their cybersecurity posture (OECD, 2012). In research by Chatfield and Reddick (2019), they highlighted the importance of forward-thinking about the adoption of emerging technologies but also emphasised the importance of complementing this with suitable cybersecurity policies (Chatfield & Reddick, 2019).

Cybersecurity measures are implemented to cater for existing threats and vulnerabilities in organisations, when organisations digitally transform, additional threats appear, and vulnerabilities are introduced which are heightened by the interconnectedness of the financial ecosystem (OECD, 2012). This introduces the view that it is not a question of “if" the organisation is not impacted by cybercrime or data loss breach, but “when” the organisation is impacted (Zurich, 2014). Cybersecurity also plays a huge role in preventing breaches and losses to organisations. Organisations are exposed to multiple cyber threats; heightened by the digital transformation strategies which is the adoption of disruptive emerging technologies, as organisations enhance their technology capabilities creating various interconnections and increasing the points of attack for cybercriminals. In research conducted by Lezzi et al. (2018), not many organisations are fully ready and have adequate or effective cybersecurity measures in place. This is due to multiple reasons such as inadequate standards, non-existent policies, and lack of consideration for cybersecurity requirements, amongst others (Lezzi et al., 2018).

Research by Macas et al. (2022), highlighted that those greater advancements in digital technologies enable cybercriminals to develop new processes to exploit vulnerabilities in adopted emerging technologies or new vulnerabilities introduced to existing technologies from the emerging technologies if not fully mitigated by the organisation. These cyber criminals develop tools that could bypass any cybersecurity controls implemented by the organisation or their third-party service providers. Therefore organisation, are not only limited to having a view of their cybersecurity posture but that of their third-party service providers as well, as a compromise at a third-party service could have detrimental effects on the organisation. Macas et al.

(2022) highlighted digital technologies such as AI could also be utilised from a cybersecurity perspective to detect attacks and analyse threats (Macas et al., 2022).

Information Technology (IT) has continued to grow, and organisations have continued to realise the importance of IT with different technologies emerging constantly. Changes happening in the technology environment are also impacting the cyber-attack surface for attackers, advancing due to the emergence of emerging technologies that are being adopted by institutions (Dimitrov, 2020).

The research by Pancholi & Strobl (2020) highlighted that the implementation of emerging technologies is a key aspect for the survival and growth of organisations, however, another key aspect is evaluating the criticality of the environment, the disruption created, and the risk introduced by these technologies, this is imperative to understand the impact to the overall cybersecurity posture of the organisation (Pancholi & Strobl, 2020). Digital transformation, specifically the adoption of emerging technologies is a critical element for organisations to develop a competitive advantage, which coupled with proactive cybersecurity measures or a proactive cybersecurity strategy, would strengthen the organisation's longevity and further heighten the ability to sustain a competitive edge. This highlights the Systems Theory of the relationship between emerging technologies and cybersecurity (Wilkinson, 2011).

2.5.3 *The overall Impact of Emerging Technologies on Cybersecurity*

Technologies such as AI and more advanced ML with deep learning capabilities have grown to become essential in the way technology has progressed, this has impacted cybersecurity both from an offensive as well as a defensive perspective; based on technologies being built by malicious cyber threat actors to gain access to systems for malicious activities such as malware attacks; while the technologies are also used in the advancements in cybersecurity to develop counter-attacking tools such as malware detection tools to defend against malicious attacks or even deep learning built into cybersecurity controls to continuous evolve by understanding the patterns of cyber-attacks (Sharma, 2021).

Cybersecurity is meant to be a means of protection for organisations' networks, systems, and data; and exists in many forms and types such as hardware, software,

and human activities, amongst others. These exist, however, in an ever-changing sphere, and in addition to the advent of emerging technologies such as cloud computing and AI, ongoing cybersecurity enhancements have become crucial to remain adaptable to the immense changes introduced by the adoption of these technologies (Macas et al., 2022b).

Emerging technologies are allowing organisations to exploit new opportunities presented to stay relevant and competitive. This, however, coupled with the interconnected financial ecosystem and the quick adoption of emerging technologies is heightening the cybersecurity challenges with new vulnerabilities being introduced through these technologies (WEF, 2022). This is influencing the cyber threat landscape which is changing at an enormous pace, and organisations are faced with the risk of ongoing cyber threats and loss of data. Cybercriminals have improved skill sets, are financially strong and in some cases funded by huge corporations, organised crime syndicates or even governments. Cybercrime continues to increase, influenced by the change in the digital landscape, with many organisations continually considering updated cybersecurity control measures to secure their data and counter the escalation of cyber incidents. The cyber threats Tactics, Techniques and Procedures (TTPs) have advanced to the point where they are difficult for standard cybersecurity measures to identify and mitigate (Sahrom Abu et al., 2018).

Organisations are faced with both internal and external threats and based on research conducted by Medoh and Telukdarie (2022), organisations are exposed to multiple threats such as viruses, worms, rootkits, trojans, spyware, vishing, social engineering, phishing, whaling, password decryption, keylogging, hacking, amongst others that necessitates an effective cybersecurity posture to counter these threats (Rosencrance, 2022). Cybersecurity requires strategic planning and prioritisation in terms of funding, resources, and procedures, as well as implementing long-term change (Medoh & Telukdarie, 2022). Attackers have emerged with greater techniques and tools able to exploit any vulnerability; institutions are required to continuously monitor and upgrade their cybersecurity control environment. Organisations need to ensure that appropriate strategies that are developed for the adoption of emerging technologies involve the relevant cybersecurity controls required to maintain an effective cybersecurity control environment (Haidros et al., 2021).

Many organisations have realised that certain emerging technologies such as AI and ML could be adopted to solve either specific or various problems about the operations of the business, for example, where applications are available as a service in the cloud or AI-powered banking applications is readily available in the same cloud environments; for various requirements including creating a single data source for customers. These solutions, however, are always vulnerable to compromise due to cyber-attacks where an institution could be exposed to a data loss breach due to inadequate or ineffective cybersecurity control measures (Chatfield & Reddick, 2019). A case in point was an incident in South Africa where a third-party services provider was compromised, leading to the leaking of sensitive financial information. There was also a government-controlled entity that was hacked leaving most of its digital environment unavailable and inaccessible (Naidoo, 2021). Events such as these have raised the importance of cybersecurity with many organisations investing large budgets to improve their cybersecurity posture. Organisations have also increased their resource capacity to deal with this heightened threat. However, despite the increased threat, organisations have not been frightened away from their drive to be digitally transformed. According to Chatfield and Reddick (2019) despite the cybersecurity challenges, organisations are still digitally transforming by adopting emerging technologies. However, the cyber threat has emerged as a critical threat to the survival of organisations with cybercriminals exploiting the weaknesses introduced when organisations adopt these emerging technologies. Organisations are faced with the experience of increased amounts of cybersecurity breaches which would inevitably influence the performance of the organisation, and in some severe instances, the existence of the organisation (Nelson & Madnick, 2017). Cybercriminals are taking multiple forms and in some cases are taking the shape of previously organised crime groups recruiting hackers to infiltrate organisations (World Economic Forum (WEF), 2022). With successful cyber-attacks, organisations face the possibility of experiencing system instability, total unavailability of systems, and loss of sensitive data, amongst others (Corallo et al., 2020).

Cybersecurity is growing and becoming one of the key challenges to digital transformation. Cybersecurity policies and standards are key components to ensure an understanding throughout the organisation as well as effective implementation. According to Corallo et al. (2020), cybersecurity measures should be incorporated into

the digital transformation strategies of the organisation. Organisations should adopt a security-by-design approach where security is included in all aspects of technology (Guggenmos et al., 2022). This would limit the multiple challenges introduced as organisations will have mature control environments or even understand the requirements to mitigate against specific or varied cyber threats. According to Guggenmos et al. (2022) cybersecurity should also be a strategic objective of organisations; and be included in all elements of the digital transformation process; and highlighted in this research is a process that is currently limited in many organisations especially when referring to a security by design approach (Guggenmos et al., 2022).

Many of these organisations have been majorly impacted by more and more sophisticated cyber-attacks such as ransomware attacks. In research from Y. Connolly and Wall (2019), it was suggested that there has been a rise in ransomware attacks impacting emerging technologies such as crypto-ransomware attacks where files are encrypted by attackers to solicit money from victims, leading to major loss exposure by various financial organisations (Y. Connolly & Wall, 2019).

In an interconnected financial ecosystem, exposure to increased cyber threats is prevalent and the resultant exposure would be exponential based on the type of attack and the value at risk; requiring financial institutions to advance their cybersecurity control measures and cyber resilience capabilities (Corallo et al., 2020). Organisations are exposed to a plethora of attacks which could impact various aspects of an organisation, it could be an attack resulting in major operational or financial losses such as a ransomware attack where a financial pay-out is demanded, it could be a phishing attack where personal data could be leaked, it could be a Denial-of-Service attack or even Distributed Denial of Service attack where the organisation’s entire network could be brought down (Byrne, 2021). In research led by Corallo et al. (2020), they noted that losses from cyber exposures varied, however, more than 50 percent of organisations that were exposed to cyber-attacks, were impacted by financial losses (Corallo et al., 2020).

2.6 The South African context

South Africa has embraced technological change in the past; with the advent of wireless technologies that also gave rise to increased cyber threats and introduced a need for increased cybersecurity. Additionally, the increased use of the internet allowed for access from any device; black swan events like the covid-19 pandemic also created a platform for individuals to connect from anywhere. For South Africa, this is not different to anywhere in the world as the threat is not different to any other country, limited cybersecurity controls or initiatives can create destruction for an institution; and when this is realised in a financial sector, impacting large systemically important financial institutions, the impact can be huge, which could cripple an entire economy (Gcaza & von Solms, 2017). Research by Gcaza and von Solms (2017), noted that South Africa is aware of the threat of cybercrime and the need for effected cybersecurity as a National Cybersecurity Policy Framework (NCPF) was approved, however, it was noted that an overall culture of cybersecurity awareness was lacking. This importance is further emphasised by the increase in internet access (Lanerolle, 2016).

Financial inclusion is another area of major concern in South Africa and emerging technologies such as digital technology and financial technologies (FinTech) give rise to financial inclusion, with the technology making it possible for all to access the internet via mobile technologies. According to Mittal (2019), Fintech institutions have grown in South Africa and have been seen as important for the growth of the financial sector due to the services they provide. These institutions were once seen as threats to the major financial organisations, however, over time that view has changed based on the realisation that partnerships between the fintech and major financial organisations would be beneficial for all parties. These partnerships introduce major benefits to both parties; however, this could be detrimental where cybersecurity was not effectively catered for in the design (Mittal, 2019).

South Africa is no different to any other country in the world, emerging technologies have both beneficial and negative effects on cybersecurity. The negative effects could lead to a considerable increase in the attack surface with the introduction of emerging technologies like cloud computing, artificial intelligence (AI), and Machine Learning (Radanliev et al., 2020). As more systems and devices are linked together, there are

more opportunities for hackers to exploit the network and systems; the growth of the Advanced Persistent Threat (APT) whereas systems become more complicated and linked, emerging technologies might give APT actors additional opportunities to exploit the systems to gain unauthorised access to either access sensitive data or even disrupt systems (Corallo et al., 2020). New unknown and complex cyber-attacks are introduced by emerging technologies where attackers could make use of AI to perform targeted attacks. While new threats are brought about by expanding technologies, there are also opportunities for cybersecurity innovation. These technologies can help organisations create sophisticated threat detection and response systems, automate security procedures, and strengthen their overall cybersecurity posture (Ukwandu et al., 2021).

Fintechs operate in different environments based on the different levels or fewer regulations that they are exposed to. Major financial institutions are looking at ways that these technologies could be leveraged to enhance financial inclusion with the financial sector playing a major part in this. This however, according to Baur-Yazbeck et al. (2019) also gives rise to increased cybercrime, influenced by the lack of adequate cybersecurity and the types of hardware technology or devices used. Institutions are also finding additional useful emerging technologies that require enhanced cybersecurity skills that are not necessarily available in the country (Baur-Yazbeck et al., 2019). Financial services are embracing the adoption of emerging technologies at a rapid pace, however, cybercriminals are also embracing this adoption and looking for gaps and vulnerabilities that can be exploited. These gaps and vulnerabilities are difficult to assess and there are heightened challenges in measuring this due to the advancements in cybercrime (Kshetri, 2019).

2.7 Theoretical Framework

The theoretical framework enables a systematic method to answer the research topic. It opens up the possibility of identifying correlations between the components in the study. It also allows for a process of creating theories from the data, abstracting key variables and identifying relationships that establish the theory (Anfara & Mertz, 2014).

Financial institutions are adopting emerging technologies at a rapid pace influencing the level of cyber exposure that these institutions are exposed to and having an adverse impact on the cybersecurity posture of institutions as well as the overall sector. It's imperative to obtain an understanding of this impact to determine if there are real benefits realisation and if this is similar across the sector. The ability to obtain an understanding is influenced by the problem of the information or lack of information to determine if there is an impact derived from the adoption of emerging technologies on the cybersecurity of financial institutions in South Africa (Macas et al., 2022).

This is a big problem as the lack of understanding of the impact of emerging technologies on the cybersecurity posture of financial institutions will increase the risk of cyber-attacks (Byrne, 2021).

Emerging technologies, such as AI, ML, and cloud computing, bring new opportunities and challenges to the cybersecurity landscape. The technology adoption is key allowing for the threat landscape to evolve. Risk management strategies should be considered within the context of emerging technologies. People play a crucial role in cybersecurity, both as potential vulnerabilities and as defenders (Hatzivasilis et al., 2020). The framework should recognise all factors involved in the adoption and use of emerging technologies, including people, processes and technologies. Given the interconnected nature of emerging technologies and their impact on cybersecurity, building overall resilience and establishing effective incident response capabilities are critical components of cybersecurity (Cirnu et al., 2018).

The questions that arise are what is the relationship between emerging technologies and cybersecurity and what is the impact of these emerging technologies on the cybersecurity of financial institutions in South Africa? With the increase in emerging technologies, so is the increase in the risk of cyber-attacks, compounded by the intricacies introduced by these technologies. This is noted extensively from an international perspective, however when looking at the financial sector in South Arica, although there is information available, the information is limited, when looking at the impact that emerging technologies have on the cybersecurity posture of these institutions. There is information pertaining to some sectors in South Africa based on a report compiled, where the increase in the adoption of emerging technologies is influencing the state of cybersecurity (PWC, 2021). The emergence of new

technologies in South Africa which is similar to the rest of the world, is introducing advanced threats and vulnerabilities that are impacting the country as a whole, with spill-over effects into various sectors (Griffiths, 2017). The use of emerging technologies such as cloud computing, AI, and ML, amongst others has advanced the cybersecurity risk in South Africa, further influenced by other associated risks such as laws and regulations amongst others, which highlight the importance of cybersecurity (Liquid Tech, 2021). With the advent of these technologies, cybersecurity has grown to be one of the most important aspects of the financial sector due to the value at risk and as the technologies advance so does the cybersecurity risk, requiring a deeper understanding of the impact on the cybersecurity posture of institutions (Hougaard, 2022). Based on this, systems theory was identified as the appropriate framework to adopt due to the perceived relationship between emerging technologies and cybersecurity.

2.7.1 *Systems Theory*

The study attempts to establish the relationship between the adoption of new and emerging technologies and the impact it has on cybersecurity to determine the influence one has on the other. Roger's Diffusion of Innovation theory was first considered for the study; however, this was mainly linked to the adoption of new technologies (Minishi-Majanja & Kiplang'at, 2013). Systems theory was viewed as the best framework to explore the impact of emerging technologies on cybersecurity; specifically General Systems Theory, that suggests the relationships between different constituents in different systems. Systems theory is built on the premise that the effect of a factor is influenced by another factor, or the factors work together to create a result (Arnold, 2013). Systems theory tries to develop a view of how aspects are related and how they influence each other, can influence each other or have a relationship that leads to the impact of one on the other. Aspects of each element can be understood in the framework of connection with each other and not necessarily individually. The theory is vital in classifying the key attributes of each component and the link between them (Wilkinson, 2011).

General Systems Theory is employed in the study; based on the idea that in addition to proposing fundamental principles guiding those interactions, general systems

theory also suggested relationships between different constituents in different systems (Arnold, 2013).

Cybersecurity is a complex system comprised of interrelated components. Systems theory aids in the analysis of the effects of emerging technologies on cybersecurity (Malatji et al., 2019).

The impact of emerging technologies on cybersecurity can be analysed and understood using the systems theory where various factors and dynamics should be considered:

- Technology Adoption
- Digital disruption
- Cybersecurity
- Threat Landscape
- Risk management
- Resilience

2.7.2 *Conclusion of Theoretical Framework*

Emerging technologies are being adopted by the financial sector in leaps and bounds creating an interconnected financial ecosystem as part of the digital transformation strategies of organisations. Because of the financial and practical issues that technology presents, the world is becoming more globally interconnected, increasing the risk of cybercrime; and requiring organisations to effectively measure the cybersecurity posture (Pancholi & Strobl, 2019). Mckenna (2021) indicated that this highlighted the additional requirements for greater levels of cybersecurity as the risk introduced due to the adoption of emerging technologies has intensified. Various trends have been observed internationally, and the importance of cybersecurity continues to rise as the level of cybercrime increases tremendously. The magnitude of technical breakthroughs, with many organisations in the financial sector adopting emerging technologies which further heightens cybercrime exposure. In research from Duc and Chirumamilla (2019), the process of evolving business and market requirements where emerging technologies are used to develop new or update

existing paradigms is taking the world by storm, which is also drastically changing the cybersecurity landscape, requiring more effective cyber strategies.

Studies conducted internationally in various jurisdictions have highlighted the massive impact that emerging technologies have on the cybersecurity posture of organisations (Griffiths, 2017).

This study delves deeper into the determination of the perceived impact of emerging technologies on the cybersecurity posture of financial institutions based on the lack of pertinent information, with the study aimed specifically at the financial sector in South Africa, including banks, insurers and market infrastructures.

By considering these elements within the systems theory, one can better understand the complex relationship between emerging technologies and cybersecurity.

2.8 Conclusion of Literature Review

Organisations adopt emerging technologies for value creation such as digital-enabled opportunities as well as rationalisation of certain aspects of the organisation, amongst others to ensure sustainability and survival over time. The success of the adoption of these technologies is based on the understanding of what the value ultimately looks like and the required strategy to achieve that. Many organisations undertake the process of digital transformation without understanding what this ultimately looks like, what the impact would be and ultimately what the risks associated with this; Cybersecurity is a critical risk based on the impact introduced by the adoption of these technologies, making organisations more susceptible to this type of risk. This is further heightened by the implementation of specific emerging technologies that create immediate change within the environment (Grahn et al., 2021). Major people, process or system changes in the organisation, requires a major increase in cybersecurity investment as well, however, according to Li et al. (2021), increased cybersecurity investments do not necessarily result in lower security breaches in organisations. Furthermore, they note that organisations that are less digitally advanced with fewer cybersecurity controls are not necessarily less susceptible to those organisations that are highly digitalised with greater investments in cybersecurity (Li et al., 2021). The result highlighted that the increased investment could lead to higher security breaches

in these digitally transformed businesses due to easier access to data via digital platforms (Rogowski, 2013).

Relevant mitigating controls are either internal or external facing controls; and breaches whether internal or external are reduced by investing in certain controls such as network controls from an external perspective whereas internal breaches are reduced by implementing other controls such as user identity and access security controls (Li et al., 2021). It is often advised that a controlled environment is only as strong as its weakest point and therefore, organisations may have the best and most expensive cybersecurity controls to complement their digital transformation, however, if there is a small vulnerability that exists, the organisation will be exposed to cyber threats (WEF, 2022). Organisations need to ensure that their transformation strategies are combined with suitable cybersecurity strategies to ensure an overall effective cybersecurity posture. Many organisations noted internationally, with multitudes of integrated systems have also adopted emerging technologies, however, not considering the additional cybersecurity risk introduced to the organisation based on legacy systems still existing in the environment (MARS, 2018). Further literature available highlights the impact that the adoption of emerging technologies has on the cybersecurity posture of organisations internationally, the literature when looking at this from a South African perspective, focused on financial institutions. Although there is some information, the level of information is limited to fully understand the overall impact.

CHAPTER 3. RESEARCH METHODOLOGY

3.1 Research approach

A research approach is defined as disparate methods of conducting research (Kothari, 2013). A qualitative research approach was employed in this study with participants from the South African financial sector, specifically banks, insurers and market infrastructures. This approach provides a deep level of information, which can also be seen as extensive descriptions; that is pertinent to the topics or issues identified in the study. Qualitative data collection and analysis techniques were adopted to conduct the thematic analysis. Systems theory, specifically General Systems theory was the framework adopted to determine the relationship between the adoption of emerging technologies and the impact on cybersecurity (Wilkinson, 2011). The participants included individuals who are involved in emerging technology-type roles as well as cybersecurity-related roles. The approach adopted for the study was based on the objective of obtaining opinions from individuals based on their experience.

3.2 Research design

Research design is defined as the strategy to obtain relevant information for the research study to address the overall research problem (Kothari, 2013). The research design approach adopted was a generic qualitative design. The approach aimed at understanding the individuals' insights, conduct and responses. The research performed was an empirical study where information was solicited based on a South African context and experience within the South African financial sector. Interviews were conducted with individuals with the required knowledge and expertise in the field of study. The research determined the current state of the impact of emerging technologies on the cybersecurity of financial institutions in South Africa. The information obtained was used to create, an overall understanding based on the population of participants.

3.3 Data collection methods

Obtaining accurate and current information was key to this study and to obtain information, the primary research method was interviews conducted in a semi-structured manner. Individuals were selected from the South African Financial Sector, specifically the banking, insurance and market infrastructure industries. The process entailed physical/virtual interviews, and documenting the interviews through transcripts, recordings, observations, etc.

The semi-structured interviews suited this study based on the ability to interview an individual physically / virtually, having discussions as well as requesting additional follow-up questions where required (DeJonckheere & Vaughn, 2019). This provided for a depth of knowledge, what is termed ‘thick descriptions’ in qualitative analysis.

The research study was exploratory in nature and the information collected from the individuals was based on their current knowledge and expertise in the specific field of study (Research at Grass Roots, 2005).

3.4 Population and sample

3.4.1 *Population*

A population is a selected cluster of individuals or objects from which the findings of a study can be derived (umsl.edu, 2022). In this study, the population consisted of personnel from the South African financial sector, specifically from the banking, insurance and Market Infrastructures industries. The purpose of this study was to determine the impact of emerging technologies on cybersecurity in the financial sector, only individuals with the required knowledge within the financial sector were considered for the population.

3.4.2 *Sample and sampling method*

A sample can be referred to as a part of the population chosen for the study (umsl.edu, 2022). In this study, the sample comprised Information technology risk and cybersecurity individuals. The sample consisted of 11 individuals. The sample size of

11 individuals was seen as sufficient based on the spread across the financial sector and the experience within the various industries. Smaller sample sizes are typically possible with qualitative research; and the ultimate goal of the research and the interviews conducted were to reach that point of saturation where the data would be the same. The individuals were from banks, insurers and market infrastructures within the South African financial sector. Some of the individuals worked across the financial sector and therefore allowed for a broader view of the questions, this played a part in the determination of the allocated number of participants.

The techniques adopted were non-probability techniques using a combination of convenience within the existing environment, purposive to obtain participants and information and snowballing to assist with additional participants or information gathering using the snowball technique, the participant will be asked to solicit additional participants.

3.5 The research instrument.

The research instrument is the interview protocol and guides the semi-structured interviews with the sample groups. The interviews were based on the primary and concluding questions included in Annexure A.

The interview protocol was peer-reviewed with input received from peers. The feedback included:

- Updating the questions to be more open-ended.
- Being specific about individuals who should be at the correct level and area of expertise to answer the questions.
- Not being too specific on the environment.

The participant information sheet is included in Annexure B and the consent form is included in Annexure C.

The questions were open-ended, which allowed for the responses to be processed and follow-up information to be asked. The approach allowed the researcher to assess the individual's body language when responding (Kothari, 2013). This same approach

was followed to determine if based on the individual body language, the individuals responded truthfully.

3.6 Procedure for data collection

The researcher approached individuals from four banks, two insurers and one market infrastructure to request interviews with experts in the field. The researcher also approach participants individually because they were known to the researcher as well-known experts in the field.

The interviews were conducted mostly using the virtual format using the Microsoft Teams platforms.

based on many organisations working from home. This was beneficial as the Microsoft Teams platform was utilised which allowed for the sessions to be recorded.

Notes were taken during the interview, however, the interviews were recorded, and transcription was enabled. The researcher asked specific questions; however, follow-up questions were asked as well. The researcher emailed the participant to advise them of the study and request participation from the participant in the study.

- The researcher followed up numerous times by email as well as with phone calls to further explain the reason for the study.
- Once the participant confirmed that they were willing to participate, the researcher scheduled the interviews.
- The compiled questions were sent to the participant to obtain a view of the questions.
- The participant was advised of the possibility of follow-up questions based on the responses.
- The interviews were conducted using the Microsoft Teams platform.
- The interviews were not more than 45 mins.
- The participants were very open and candid with their responses.
- The participants did offer follow-up meetings if required.

3.7 Data analysis strategies and interpretation

For this study, a Thematic analysis was utilised similar to the process given where in a qualitative analysis, holistic, overarching ideas and views were derived (Braun and Clarke, 2006).

In research from Braun and Clarke (2006), various aspects were noted to follow, to perform the data analysis.

- Create an overall understanding of the information.
- Arrange the information in a structured manner.
- Determine the specific ideas or overarching views.
- Analyse the ideas and views and determine if they can be updated or changed.
- Create explanations for these ideas and views.
- Compile the research paper.

3.8 Possible limitations and challenges of the Study

Some limitations were noted for this study. The timelines were limited to 3 months based on the late ethics approval received; and based on the timeframe, the study was purely qualitative. The sample size was dependent on the acceptance from participants; the responses from participants delayed the process further. Participants targeted were limited to the banking, insurance and market infrastructure sectors. The interviews were conducted virtually.

3.9 Quality Assurance

3.9.1 Dependability

The study investigated the impact that the adoption of emerging technology has on cybersecurity in the South African financial sector. This was validated with data received through semi-structured interviews with experts in the field and the industries and re-checked with the same experts throughout the interviews.

3.9.2 Credibility

The questions were closely related to the main research question. The same questions were asked in different interviews with different individuals to triangulate the responses to verify the consistency of responses. The participants were able to provide more information and not just that was asked by the interviewer.

3.9.3 Transferability

The information is related to the financial sector based on the sample and the sampling methods, however, its assumed that the information is transferable to different contexts.

3.10 Ethical considerations

The process to obtain consent to interview employees of companies where required or to use company information was followed, individuals were requested to respond whether they agreed to be interviewed. The research was taken through the University for ethical clearance. Each participant provided consent and responded yes to the question in the recording as well. Participants were advised of the process to ensure anonymity by removing any reference to the participants names and company names and also ensuring the information was store on an encrypted drive.

3.11 Proposed schedule and timelines

The timelines of the study were limited to six months, however, that was further reduced to 3 months because of the late approval from ethics and further reduced because of the delayed responses by the participants. A portion of the time was utilised for interviews; the remainder of the time was utilised to analyse the information; verify the information; and then finalise the report.

CHAPTER 4. PRESENTATION OF RESULTS

4.1 Introduction

The outcomes of the research are presented in this chapter, focusing on the findings based on the data collection. The data was gathered from semi-structured interviews with senior management and experts who have been or are involved in the information technology, digital, risk management and cybersecurity field. The questions solicited the level of adoption of emerging technologies and the understanding of those technologies. Moreover, the questions also sought the understanding and adoption of emerging technologies, the current cybersecurity posture and the impact that emerging technologies have on cybersecurity in the South African financial sector.

The chapter focuses on the qualitative analyses of the data received.

4.2 Profile of respondents

4.2.1 *Position and Sector*

The respondents were from the financial sector and were directly linked to technology risk and cybersecurity roles, specifically in the banking, insurance or market infrastructure industries.

Participant	Position	Sector
1.	Chief Information Security Officer	Insurance
2.	Chief Information Security Officer	Bank
3.	Senior Information Security Manager	Bank
4.	Chief Information Security Officer	Bank
5.	Head of IT Risk	Bank
6.	Senior IT Risk Manager	Bank
7.	Chief Information Security Officer	Bank

8.	Head of Information Security	Insurance
9.	Head of Legal Risk and Compliance	Market Infrastructure
10.	Chief Information Security Officer	Market Infrastructure
11.	Chief Information Officer	Market Infrastructure

Table 2 Participants

4.3 Qualitative Results

The research questions considered for the qualitative study focused on the impact of emerging technologies such as AI, ML and Cloud technologies on cybersecurity, in the financial sector.

The main research question for the study:

- What is the impact of emerging technologies on the cybersecurity posture of financial institutions in South Africa?

The research sub-question:

- Is there a clear relationship between emerging technologies and cybersecurity?

The overall interview questions were open-ended, allowing for open discussions with many of the responses being interrelated to each other. There were widespread responses, however, all of the participants were aligned in terms of their views on both emerging technologies as well as cyber cybersecurity. The questions and answers were considered and analysed from the recorded interviews conducted and the transcripts obtained.

The thematic analysis method used was adopted according to the six-step process as highlighted by Braun and Clark, (2006) which entailed:

Understanding the information.

1. Developing codes from the information.
2. Developing themes from the codes.
3. Verification of themes developed.

4. Defining the Themes.
5. Finalising the analysis.

A key element for the analysis was that although the process adopted is reflected as a phased, simultaneous approach, it was iterative, where the process was repeated multiple times until a point of comfort was achieved (Braun & Clark, 2006b). The process starts with a key understanding of the information that was gathered from the interviews; analysing the information to apply codes to the information; followed by combining the codes into overall themes; and finally creating an overall view of the analysis.

4.4 Thematic analysis

Thematic analysis is the process of sourcing data, reviewing and analysing that data and then highlighting themes or patterns from that data (Braun & Clark, 2006). The process to analyse the data obtained from the interviews held are depicted in Figure 3 below. The transcripts were analysed, and codes were identified from the data. A combination of a manual process as well as the use of the Atlas.TI tool was used to analyse the data. Each participant's transcriptions were uploaded to the application, where they were examined. The procedure of analysing the transcribed document involved listening and reading the interview, picking out the most important participant input, and then classifying the feedback into groups based on comparable meanings. This was than manually linked to these corresponding groups in the form of coding. The codes were strongly linked to the data and were classified into descriptive codes based on the data received and then linked to overall pattern codes that were derived from multiple descriptive codes as part of the inductive coding process (Creswell, 1998). The inductive codes were compared to the prior developed deductive codes. These codes were then analysed further to identify emerging codes. The emerging codes were then analysed and linked to overarching themes that were defined from the data collected (Miles & Huberman, 1994). These themes were derived based on the overarching data and were then reviewed and defined. Similar data was linked to the same themes or sub themes. The figure below highlights the overall process that was followed from the analysis of the transcripts to the definition of the themes. The

data was scrutinised, linking each question and response, identifying the similarities and disparities.

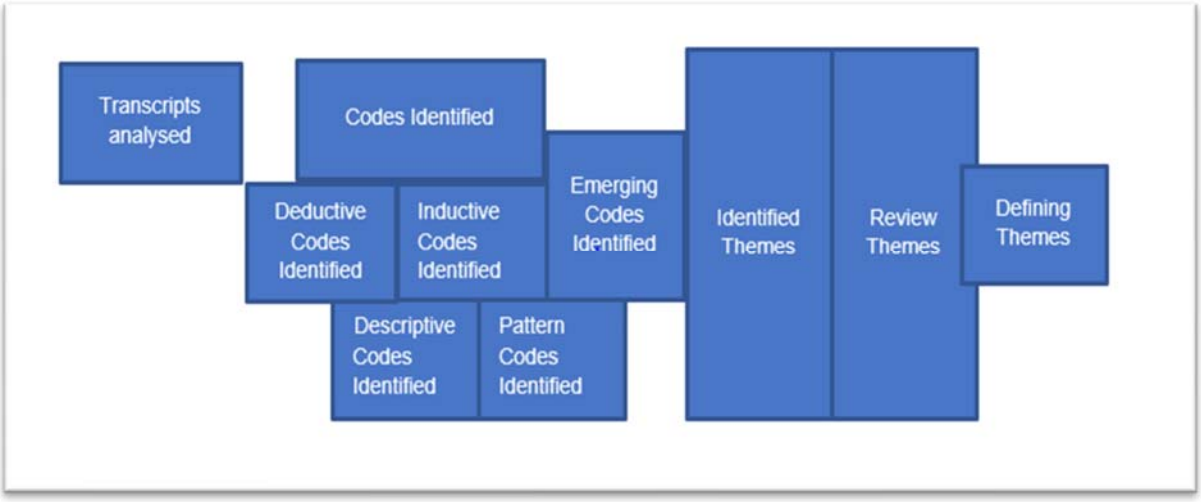


Figure 3 Thematic analysis for research

A review of the transcripts was conducted, including going through the recordings to conduct a thematic analysis of the responses to derive relevant codes. The coding process involved the identification and description of various codes.

4.4.1 *Coding*

Deductive Codes
• Knowledge of emerging technologies. • Digital Transformation strategies. • Cybersecurity maturity. • Cybersecurity requirements. • Identification and mitigation of cybersecurity risks. • The effects of emerging technologies.

Table 3 Deductive codes

Inductive Codes	
Descriptive Codes	**Pattern Codes**
• Emerging or new. • Cloud technologies. • Machine learning.	New technologies.

• Artificial intelligence. • Large language models. • Quantum computing. • Post-quantum crypto algorithms. • Crypto Assets. • Digital Ledger technology. • Robotic process automation.	
Description of Pattern codes	
New type of technologies are predominantly adopted by financial entities; or new technologies that are different and continuously evolves.	
Descriptive Codes	**Pattern Codes**
• Digital adoption. • Application Programming Interface (API). • Transforming, emerging, and changing strategies. • Automation.	First in digital.
Description of Pattern codes	
The fourth industrial revolution; attributes highlight the focus on digital by financial entities. Optimise the customer experience. The new frontier or the new Revolution of technology.	
Descriptive Codes	**Pattern Codes**
• Aggressive. • Experimental.	Take-on strategies.
Description of Pattern codes	
The level of adoption of digital technologies by the entity.	
Descriptive Codes	**Pattern Codes**
• Zero trust technologies. • Threat casting. • Threat Intelligence. • Control capabilities • Red teaming.	Cybersecurity control environment

• Detection technologies. • Software Development Life Cycle. • DevSecOps. • Control environment. • Monitoring of networks.	
Description of Pattern codes	
The cybersecurity control environment.	
Descriptive Codes	**Pattern Codes**
• Threat Landscape. • Emerging threats. • Threats and vulnerabilities. • Social engineering. • Threats and opportunities. • Change in the threat landscape.	Cyber threat landscape
Description of Pattern codes	
The cybersecurity threat landscape.	
Descriptive Codes	**Pattern Codes**
• Structured risk assessment. • Strategic risk planning. • Cyber hygiene practices. • Awareness and training. • Automated penetration test. • Security Operations Centre.	Cyber risk management.
Description of Pattern codes	
The cyber risk management function.	
Descriptive Codes	**Pattern Codes**
• Deployment of EDR. • Security Operations Centre. • Additional monitoring. • Response procedures. • Incident response plans. • Application security framework.	Ability to adapt and respond.

• vulnerability scanning. • Cyber security maturity. • Control redesign. • Immature with cloud adoption.	
Description of Pattern codes	
How entities adapt and respond.	
Descriptive Codes	**Pattern Codes**
• Detect anomalies. • Behavioural analysis. • Automation to increase or reduce our response time. • Threats in multi-cloud type environments. • Digital banking fraud. • Zero-day attacks. • Attack surface. • Third-party risk. • Data exfiltration.	Impact of the technology.
Description of Pattern codes	
The impact of emerging technologies on cybersecurity.	

Table 4 Inductive codes

Deductive codes were developed prior to the review or collection of the data. The data was then carefully analysed and descriptive and pattern codes were developed. The inductive codes which are a combination of the descriptive codes and the pattern codes were compared to the initial descriptive codes that were developed before any of the data was collected to derive the overall emerging codes.

The emerging codes were then reviewed and linked to overall themes based on the data that was received and analysed from the semi-structured interviews conducted.

4.4.2 *Emerging Codes and Themes*

Emerging Codes

• Emerging Technology. • Digital Transformation. • Cybersecurity Posture and Controls. • Cybersecurity risk assessment and mitigation. • Ability to adapt and respond. • Impact of emerging technologies on cybersecurity.
Themes
The below themes were derived from the overall coding process.
• Emerging Technologies and its Adoption. • Digital Transformation Strategies. • Cybersecurity Posture and Controls. • Cybersecurity risk assessment and mitigation. • Impact of emerging technologies on cybersecurity. • Ability to adapt and respond.

Table 5 Emerging Codes and Themes

4.4.3 *Defining the Themes*

The interviews conducted created emphasis on the themes that were drawn out of the data. There were similarities noted across the interviews that assisted in the coding process as well as in identifying the themes and ultimately defining the themes based on the data. There were multiple themes that were identified; however, these were consolidated into six themes that were derived; however, they were further reduced to three main themes and three sub-themes linked to each main theme. These themes were focused on the main aspects of the paper, being emerging technologies, cybersecurity and the impact of these technologies on cybersecurity. These themes allow for the triangulation of information in terms of what was derived from the literature, what was derived from the interviews and the recommendations.

- **Theme 1:** Emerging Technologies and their Adoption - newer or unknown technologies, adopted at various levels and speeds within the organisations.
    - **Sub-theme 1.1:** Digital Transformation Strategies - the drive towards digital emerging technologies as well as digital businesses within each organisation.

- **Theme 2:** Cybersecurity Posture and Controls - the level of cybersecurity maturity within the organisation and the types of controls implemented.
    - **Sub-theme 2.1:** Cybersecurity risk assessment and mitigation - the overall risk management process and cybersecurity controls implemented within the organisation to manage and mitigate cybersecurity threats as a result of emerging technologies.
- **Theme 3:** Impact of emerging technologies on cybersecurity - the result of implementing new technologies and the effect it has on the cybersecurity control environment of the organisation.
    - **Sub-theme 3.1:** Ability to adapt and respond - the ability of the organisation to react to and continue with business as usual in the event of any attack, incident, breach, etc. that was heightened due to the impact of emerging technologies on cybersecurity.

4.4.4 *Interview results*

4.4.4.1 Theme 1: Emerging Technologies and its Adoption

With regards to emerging technologies and their adoption; participant .1 (part. 1) highlighted that the adoption was fairly aggressive, however, for certain technologies such as cloud technologies, the initial approach was cautious based on the cost factor. Part.1 did, however, note that referring to cloud computing as an emerging technology might be an error because it's been around for a long time; rather, the technologies that are top of mind for most people when talking about emerging technologies were AI and ML. Participant .2 (Part. 2) noted emerging technologies as new technologies that are different from the current technology that is being used and also highlighted AI and ML as technologies where big strides were being made. Participant .3 (Part. 3) has a similar view and referred to emerging technologies as technologies such as AI, ML, cloud computing, etc. and highlighted that these technologies were being adopted fairly fast in the organisation as there is a fear within the organisation of falling behind the curve. Participant .4 (Part. 4) had an interesting view that the world is constantly changing, and technology has been emerging and changing for a long time as well, however, technologies such as AI and ML, are going to create a different reality to what we see now. Participant .6 (Part. 6) highlighted that emerging technologies are

those technologies with major benefits that can be offered with the proper use of them, e.g., AI and ML, however, it's not yet known how to apply these technologies. Participant .11 (Part. 11) referred to emerging technologies and their adoption of them in terms of what the business needs, like platforms that are relatively new or emerging technologies like the cloud platform.

4.4.4.1a Digital Transformation Strategies

Digital transformation strategies were noted to be strongly linked to emerging technologies. Part. 1 advised that there was a big drive within the organisation to create better customer experiences and to unlock different types of products for different market segments using digital technologies, however, it was noted that this was creating major disruptions in the industry as a whole. Part. 3 highlighted that the strategy is all about being first in digital to create that added value for the customer. Part. 4 emphasised that digital strategies are usually very vague but what it means in the organisation is being very deliberate about the customer first and in many cases. A large portion of the business processes requires rethinking and then using technology to make them more efficient. So that's where digital transformation or digital strategy is coming into play within the organisation. Part. 5 noted that digital transformation is not necessarily the same for each organisation because some organisations might be much further ahead than others. Some organisations might have a lot of legacy systems that need to be updated or go through a process to digitise those systems – "*Digital strategy is very much integrated into our overall IT strategy. It is not something that stands separate because we're not in a situation where we have to convert massive legacy environments" (Part. 5).* Part. 7 noted that digital was changing the landscape and it's becoming imperative to ensure that everything is available on digital platforms and channels.

> *"We don't want to have any additional unwanted admin, clients shouldn't have to do anything else they don't need to, you can stand in a queue at one of our ATMs as half the country does at any one point in time, you can come into your branch and be serviced, but you should be able to do all of those things other than get cash out of your phone. And we obviously want to move people away from cash. Should be able to get everything from the app on your phone without*

the need for any of those other support services around" (Part. 7). This extract highlighted the drive by the institution towards digital transformation; a reflection shared across the financial sector.

Part. 8 noted the digital strategy was driven from an IT enterprise architecture perspective, hence the IT security architect was involved; so, the IT enterprise architecture provides the services to assess any new technology trends identified by relevant suppliers and ensure that these new technologies are integrated into the overall. Part. 9 highlighted that to fully explore digital transformation, you need to understand the organisation's footprint. The organisation views digitisation in the sense that everything currently done in the business is digital. Part. 9 noted that the organisation deals with a plethora of transactions every day and that a lot of reconciliation must also be done about the significant amounts of transactions that pass through the systems. Therefore, manual execution is essentially not an option, and as a result, the foundation of the organisation is the adoption of digital technologies that allow the business to accept transactions.

4.4.4.2 Theme 2: Cybersecurity Posture and Controls

When discussing the Cybersecurity posture and control environment, part. 1 noted that the organisation's cyber posture was fairly mature. This was assisted by the fact that traditionally hosting of the organisation systems was mostly on-premises. The control for on-premises hosting is fairly mature and working well. Part. 1 noted that they were still immature with the cloud, that is also because the adoption of the cloud within the business wasn't necessarily that fast. Part. 3 highlighted that the entity was comfortable with its security posture and a lot of focus was given to independent assessments as it was quite important for the organisation to get a view of the maturity. Various self-assessed views are obtained of where the organisation is in terms of posture. The organisation has a very good track record in terms of cyber security, in terms of keeping systems safe and secure.

"*We've been talking about digitisation, all of this new stuff. It does expose you; it does extend the digital footprint that you have, and you need to be wide awake to every setting that you have and configuration that you do in this sort of environment. We are still not where we want to be but definitely an improvement from the previous assessment" (Part. 3).*

Part. 4 highlighted that cyber security is about risk management as a start within the organisation. The organisation defined the cybersecurity posture based on how risk is assessed within the organisation. Triggers were added where amber is an indication of an increasing improvement trend. This means the cybersecurity posture is at a place where some work has to be done to improve.

> *“Since we are very sceptical of ever claiming to be "green" in cyberspace, cybersecurity threats will always exist. Depending on the threat actors and the shifting nature of the cyber world in which we live, the controls we put in place will need to increase or decrease” (Part. 4).*

Part. 5 had a similar view and noted that the entity had a very strong tone at the top when it came to risk management. Part. 6 emphasised that the cyber posture of the organisation is fit for purpose, tested regularly, and it is effective. It about was always asking what doesn't work if the current controls work not and ensuring processes and mechanisms to rectify if it’s required. Part. 7 referred to the cybersecurity posture as well respected and understood. *“You know, Cyber is a first straight citizen inside the organisation. We get access to all the committees and things like and people that we need” (Part. 7).* Part. 8 highlighted that the posture is always maturing. Part. 10 highlighted that the cyber footprint was very unique in the sense that the organisation does not hold retail accounts, and the organisation does not transact any business on an online platform.

> *“Our website for example is very removed from our critical infrastructure; so, our footprint is very small. You know the number of connections into the environment is less than 200 and all of them are known. However, the reason it's such a big issue in our world is because of the strategic importance of what we do. If we stop, if we have any impact on operational activity, it means that no settlement will happen in the country on that day. So, for us, it's a big issue because of the strategic importance of our function, not necessarily our footprint which is very limited. But I'm comfortable in with regards to the response that wants to give it's very mature” (Part. 8).*

These extracts highlighted the awareness of the entity towards digitisation and the cyber threat as well as the required posture; a reflection shared across the financial sector.

4.4.4.2a Cybersecurity risk and vulnerability management

Cybersecurity risk and vulnerability management were strongly linked to cybersecurity posture and part.1 highlighted that there are a lot of informal engagements where new technologies are being considered within the business. The cybersecurity function within the business gets invited to meetings, however, it noted that that's not full proof, so a formal process was developed where nothing that is invested in or deployed on the network is allowed to be approved if it doesn't go through the approval process and as part of that process, from a cybersecurity perspective, members from the cybersecurity team as well as the security architects are involved. This also leads to ad-hoc almost structured risk assessment like for emerging technologies. Furthermore, part.1 noted that the identification and assessment of cyber security risks are not different from the existing process, and it was included in the strategic planning. The strategy document refers to threats and opportunities and forces that drive decisions, which would include emerging technologies. "*So, 4-5 years ago we already started talking about what the impact of artificial intelligence would have been or could be in the future for us" (Part. 1).* Part. 2 noted that the adoption of new technologies would typically follow a new project being registered including the security evaluation of the technology that is planned to be onboarded. The cyber security measures are assessed each time these new technologies are implemented. Part. 2 highlighted that for the immediate mitigation actions if cybersecurity risks are identified, typically a joint operation centre is established where the technical analysis of incidents is done and then escalated if needed. Part. 4 highlighted that they defined certain risks that can emanate from technology and external cyber risks:

> *"We have a table we call it the top ten, top 11 risks right now and we continuously monitor our external threat environment, the intelligence we get to see how these risks have gone up or down based on the threats that are out there" (Part. 4).*

Part. 5 mentioned that the threat Intelligence team sometimes look at new and emerging technologies and what they can find in resources, in terms of threats and vulnerabilities for new technologies. If the business or other IT teams did not discuss the new technology that they want to apply from a cyber perspective with the architects upfront, there is a catch point where the cyber team can test for vulnerabilities and ask questions if they are not involved and advise if it needs to go back to the drawing board

from an architectural standpoint. Part. 6 highlighted that cybersecurity risk and vulnerability management is referred to as centres of mastery, where cyber risks and IT risks are assessed. The organisation has done a lot of work over the years from the cyber team's perspective and the risk management perspective to educate the solutions architects to ensure that they know what to look for and how to design with security in mind. So, it's more of an empower and educate approach from a design perspective.

Part. 7 highlighted that risk offices or Information Security Officers get involved with new designs and new applications that want to go live and interact with the architects. There are cyber architects on call to help with integrating cyber architecture into application architecture. The cyber specialists will get involved through the various ways to put together the standards or patterns that are being adopted. Part. 8 mentioned that with emerging technologies, that's where the increase in the back and forth is noted. The organisation has a standard server security assessment that is undertaken, regardless of the technology, whether new or old, the standard server security evaluation is conducted, which is also risk oriented. Part. 9 highlighted that the technical nature of cyber requires adequate training.

> *"We had a new technology being introduced into our ecosystem and we've been looking at alternative methodologies for training staff. So, in our space that would potentially be a new technology or at least the provider is introducing new technology into our space, which will enable e-learning" (Part. 9).*

Part. 10 highlighted that in terms of the governance structures, whether you have a new component, or a new piece of software being introduced into the organisation, they would go through a change management process where that involves a new tool especially or a technology that's not in use in the business that also goes through the Cyber and Data Security committee so that new technology would be interrogated there. Part. 11 noted that the entity followed a risk-based approach with relevant tools already in place.

These extracts highlighted the need for effective cybersecurity risk and vulnerability management and the awareness that is linked to the cybersecurity posture of the organisation.

4.4.4.3 Theme 3: Impact of emerging technologies on Cybersecurity

This is the main theme of the research and is linked to both the main and the sub-questions. When discussing the overall impact, part. 1 mentioned that there might be more opportunities created rather than risks, although cybersecurity controls have to be constantly assessed. Opportunities are created in many aspects with big data and machine learning capabilities able to allow for better detection of anomalies. Part. 1 mentioned that a lot of effort is invested into third-party tools that make use of Artificial Intelligence that focuses on behavioural analysis, picking anomalies from potential suspicious behaviour and things like automation to increase or reduce response times by automating. Part. 2 advised that the impact is complex because the current technologies and the security technologies have many emerging technology integrations changing the threat landscape as well as the attack surface. Organisations now have the potential of AI being used to do attacks on financial systems and learning to impersonate through AI. Part. 3 also highlighted that the attack surface is constantly changing, however, noted that there are constant things that are being looked at such as whether technologies are following the correct standards. *“It’s agreed what's the gold standard that we want to apply and then technologies that come with capabilities and toolsets that you then actually adopt, and they improve what you have the way that you manage your security” (Part. 3).* Part. 4 highlighted that we are living in a connected world where organisations can control their internal environment from a cyber perspective but noted that the risk is where they cannot control external entities that they interact with, and threat actors are beginning to understand that. Part. 4 noted that the supply chain attacks are a good example where the increase or data exfiltration is being seen through third parties or small businesses that have the organisation’s data but are not investing in their cyber controls the way that they should be. It was also highlighted that people are also a major factor as you will still find people making mistakes; this is where technologies like AI, and ML can help. It needs to be able to, just like threat actors are using it to create better attacks. Part. 5 noted that from an overall control environment perspective, the technologies are mature. It’s accepted that with the emergence of new technologies and digital, certain controls are just going to become ineffective. The control of having decision trees and having manual follow-up on alerts are already ineffective or inadequate to some extent because there are products that can alleviate

that alert fatigue that can tag the human out of the process and start reading out potential faults. "*Redundant or ineffective because of technology, it's evolving as technology evolves. You going to find things that work today or are ineffective or inefficient tomorrow because of technology" (Part. 5).* Part. 6 also noted that technology is constantly evolving, and the impact would render the technology worthless. Part. 8 highlighted that the risk exists and has the potential to break many things including the many encryption methods that are used to protect sensitive data. Quantum computing is also an emerging technology and one that actually can introduce many other cybersecurity threats. Part. 9 emphasised that the impact was twofold:

> *"On the one hand, I think one needs to guard themselves against trying to adopt new technologies because it's the flavour of the month, so to speak. I think that when an organisation decides to adopt a new technology, they need to be a strong case for that technology in terms of how it creates efficiency or how it enables the organisation. Sometimes I think that your current technology may be fit for purpose, and you don't need to upgrade it after you've done the appropriate assessment if your technology is fit for purpose, then I would like to assume that your cyber defences have also been designed to give you resilience from the cyber perspective if your new technology or there is a need to adopt new technology in your environment" (Part. 9).*

Part. 10 highlighted that cyber security practices are not cast in stone. There is a need for them to be adaptable and to be able to be moulded to manage any sort of identified emerging threats. Part 10 noted that there is a need to be able to adapt as you move along as it's quite critical and something that the business is cognisant of. Part 10 highlighted that another key aspect for the organisation and especially around emerging technology is that there's a need to look at the environment and look at threats that are seen in the environment. Part. 11 mentioned that the impact was big, however, the entity does have a cyber security committee where emerging technologies are discussed and is always a standing agenda item. This is how it's practically discussed, and updates are provided on how the organisation is doing from an emerging technology point of view. Part. 11 mentioned that internal and external auditors are also involved to provide a view. This is key to getting different views on how the organisation is performing and how other organisations are doing through the ecosystem.

Thes extracts highlighted the impact of new technologies on the cybersecurity posture of organisations and the need for all organisations to remember that cyber is something that is ever evolving and whenever something new is introduced from a technological perspective, cyber has to be top of mind.

4.4.4.3a Ability to adapt and respond

This sub-theme is closely linked to the main theme on the impact that emerging technologies have on cybersecurity, and further highlights the ability of the entities and sector to recover. Discussing the organisation's ability to adapt and respond, part. 1 felt that the entity was able to adapt and respond and noted that.

> *"The fact that we are, well up till now been fairly cautious, made our jobs a bit easier? But we have in the past when ransomware became a big problem, we managed to get approval and get deployment of Endpoint Detection and Response (EDR) really within a very short space of time" (Part. 1).*

Part. 1 thought that it was imperative to keep the relationship with Group executives, Senior managers in the business units as well as the board abreast when serious risks are identified to ensure the necessary response, focus and attention that is required. It was highlighted that a key challenge that affects the organisation's ability to adapt and respond is the lack of experience in certain areas like multi-cloud type environments, the monitoring and response side in a hybrid and multi-cloud setup is still a concern. Part. 2 had similar concerns, however, highlighted that the entity was able to adequately adapt and respond. Although, there are a lot of activities including reviewing integration with existing systems and the resulting issues that can be created. Part. 3 highlighted that the entity was able to adequately adapt and respond because the teams are so close to what was happening in the environment. This is enabled through additional information that goes into the SIEM (Security Incident Event Management) and into the SOC Security Operations Centre environment. Part. 4 felt that the entity would *"absolutely"* adapt and respond to new cybersecurity threats introduced by these emerging technologies. Part. 5, 6, and 7 noted the ability to adequately adapt and respond, with part. 5 highlighting that *"we very good at swarming around things and responding to things".* Part. 8 noted that if you look at the pace of the risks introduced due to emerging technologies versus the current cyber security controls or incident response plans that you may have, it's becoming very difficult and

creating a lot more caution. The level of security for the environment or solution is a lot a concern,

> "Taking *one key example, you move everything to the cloud, but there's an opportunity for misconfiguration or there could be access management requirements that have not been configured accurately. So, you find that even those cloud solutions or your service providers bring their security modules and if you want to have security, you must purchase this module from the cloud provider. So, the cloud provider sells this, but they say well if you want to add more security, you have to purchase another module, so from a cost perspective that's when it becomes a problem that's created" (Part. 8).*

Part. 11 noted that the entity has got a very mature response and detection capability with 24/7 monitoring and alerting which highlights whenever there is something new in terms of zero-day exposure. *"If there's a zero-day malware or whatever the case is, we do get alerts on those and we are also able to respond. We respond by limiting the impact if there is any. We have very simple ways of responding to it and then later on implement that corrective measures when we do have the time" (Part. 11).*

The extracts highlighted the need for organisations to be ready to adapt and respond to the cyber threat, regardless of the technologies implemented; A view shared across the sector.

4.5. Results Summary

Chapter 4 highlighted the key results from the data collection process. Braun and Clarke's (2006) thematic analysis process was used in the framework of this study to identify codes and themes from the interview data. Three main themes with three sub-themes emerged from the data. These Themes will be analysed and discussed further in the next chapter, chapter 5.

CHAPTER 5. INTERPRETATION OF RESULTS

5.1 Introduction

The chapter looks at the analysis of the interview data guided by the three main themes and three sub-themes that were derived from the data. The themes are related to the research questions that it answers and the responses from the data to align with the systems theory and highlight the relationship between the adoption of emerging technologies and the impact it has on cybersecurity. Theme 1: Emerging Technologies and its Adoption, with a sub-theme: Digital Transformation Strategies; Theme 2: Cybersecurity Posture and Controls with a sub-theme: Cybersecurity risk and vulnerability management; and Theme 3: Impact of emerging technologies on Cybersecurity with a sub-theme: Ability to adapt and respond. The themes are individually linked to the question that it answers.

- **The main research question for the study:**
    - What is the impact of emerging technologies on the cybersecurity posture of financial institutions in South Africa?
- **The research sub-question:**
    - Is there a clear relationship between emerging technologies and cybersecurity?

5.2 Theme 1: Emerging Technologies and its Adoption

This theme intends to determine the view of the sector in terms of emerging technologies i.e., what does the sector refer to as emerging technologies and to ascertain the level of adoption. The aim is to answer the main research question.

Theme one captures the view that emerging technologies are new technologies that are different from the current technologies that are being used within the industry and sector. Technologies are constantly emerging; these technologies may not necessarily be new but could be referred to as technologies that exist and demonstrates some level of efficacy and efficiency that may then be tailored to the environment (Part 9).

The adoption of emerging technologies was largely noted as aggressive across the sector with the view that the world is ever-evolving, it's always transforming, emerging, and changing; it hasn't been static for a long time and is evident in the digital age that we see right, which could be referred to as the adoption of cutting-edge or bleeding-edge technology (Part 4). Vial (2019) noted that there was an increase in the adoption of emerging technologies such as cloud computing, Artificial Intelligence (AI) and Machine Learning (ML). Some technology was noted as something that has maybe been around for a few years but not matured in the environment. Top of mind when emerging technologies were discussed with the participants were artificial intelligence, machine learning and cloud technologies. Although it was noted that referring to cloud technologies as emerging could be a mistake because it's been around for a while. According to D. Xu (2010), cloud computing was a new catchphrase for a while in the information technology industry. It was a new technology that received a lot of attention from scholars, researchers and the industry. It was expected to contribute to a better more efficient way of providing, supporting and managing products and services (D. Xu, 2010). Cloud has emerged in some instances and although the view that it's no longer emerging, the technology has evolved and many organisations have adopted these technologies, many still view it as emerging. There is many different types of emerging technologies, however, most of it is focused on what the organisation is familiar with, how the business operates, where the business objectives are, and where the organisation is moving in terms of its strategic objectives. Organisations have implemented disparate technologies with some looking at platforms that are relatively new or emerging including cloud platform expansions (Part 11).

There were many variations of AI and ML noted and the potential of using more advanced AI such as large language models like ChatGPT and BARD. AI was noted as definitely growing exponentially, however, also giving rise to newer emerging technologies such as quantum computing. Many quantum computing researchers and AI researchers believe that there have already positive connections noted between the combination of the two technologies in the form of machine learning. This will add a different dimension to the adoption of technologies (Ying, 2010). However, many noted this as creating massive changes to the cyber threat landscape. Most organisations are on high alert with the constant introduction of new and emerging technologies that could create different challenges (Part. 1). There is a strong view

that there is a major benefit with the combination of quantum computing and AI, however, there are also major risks that can be introduced (Part 8).

The increased adoption of machine learning in the sector has seen a lot of excitement around the potential benefits across multiple functions. Technology has been constantly evolving, that's the nature of technology, however, the advent of AI and the growth of machine learning is something that can take organisations, sectors and Industries to a new level (Part 4). This is also creating a lot of uncertainty and the sector is not entirely sure of the true capability of the technology, both from a positive and a negative perspective. Furthermore, this view is enhanced by the fact that this is no longer research, but reality (Rodrigues et al., 2022).

5.2.1 *Sub-theme: Digital Transformation Strategies*

This sub-theme is linked to theme one and the intention is to determine what level of emerging technologies is related to digital transformation and the adverse impact it has on organisations and within the sector. The aim is to answer the main research question.

Digital transformation is referred to as an enabler in terms of growth, part of the fourth industrial revolution with an additional focus on changing from monolithic systems that were built for a certain capacity and modernising the architecture. The process of transforming, emerging and changing the technological landscape of organisations, sectors and industries at large. The advent of the digital age with rapidly growing digital technologies, changing the way people, process and technology interacts (Randanliev et al., 2020). There's a fairly big drive to use digital technologies to optimise the customer experience, i.e., create better experiences, understand the pain points of customers, and unlock different types of products for different market segments. This is enabled through more aggressive digital strategies, influenced by the fear of falling behind the curve or being seen as laggards in the sector; being first in digital (Part. 3). The advances in digital have changed the way organisations are structured, creating a plethora of opportunities, and enabling different avenues of business, but also creating risks. According to Randanliev et al. (2020), this growth could also affect smaller and medium type businesses as they may not be in the same position to adopt these technologies in the manner that the larger organisations would; whether due to

a lack of skills, exorbitant costs, etc., moreover, creating a bigger gap between the larger and smaller entities (Radanliev et al., 2020).

Digital transformation has seen a growth in the collaboration between organisations and fintech businesses often due to fintechs' ability to quickly provide the know-how or skills required for digital emerging technologies (Rodrigues et al., 2022). There has also been a change in strategy where organisations have transformed a portion of the business to operate as a fintech-type business. Many financial organisations have set up fintech type business models or even entered into partnerships with service providers that operate almost as fintech similar (Part. 1). According to Rodrigues et al. 2022 experts are having difficulty evaluating the impact of each player's activities and the various parties involved in a more digital environment in which data and information are shared. Fintech companies are unquestionably fresh entrants into the sectors and industries. However, no rules can yet be applied to these entities, however, organisations may struggle to digitally transform on their own (Rodrigues et al., 2022).

The consensus is that Digitisation is real and happening with many organisations forced to digitise because of legacy systems or technical debt in the environments, others because of the fear of not staying current or relevant to compete, or even to change from old monolithic systems that were built for a certain purpose. The fear is that if organisations don't adapt, they will fall behind (Part 3). This creates the term digital disruption within the sector. According to Stewart et al. (2016), digital technologies have the power to significantly change how institutions operate and this has already been extensively demonstrated. Digitisation is increasingly challenging why organisations exist and what basic value they bring, rather than simply improving how they perform. This digital disruption phenomena is accelerating and becoming a serious threat to most organisations, sectors and industries at large, forcing organisations towards adopting digital and other emerging technologies to ensure survival (Stewart et al., 2016).

Digital transformation together with other emerging technologies is seen as an enabler in terms of growth for the business (Part 10). According to Chatfield and Reddick (2019), there are opportunities to create new trends, niche markets or competitive edge Chatfield & Reddick, 2019).

5.3 Theme 2: Cybersecurity Posture and Controls

This theme intends to answer the sub-question, trying to determine the changes in the cybersecurity control environment based on the relationship derived from the changes due to emerging technologies.

The cybersecurity posture is viewed disparately across the sector; however, the level of maturity is often assessed in the same way using similar processes. The cybersecurity posture is influenced by changes in technology, either creating control gaps or in some cases rendering controls obsolete. According to Lezzi et al. (2018), cyber threats are exacerbated by the adoption of disruptive emerging technologies (Lezzi et al., 2018). Technological advancements like the adoption of AI and ML require a constant assessment of the cybersecurity posture and control environment as its constantly changing (Part. 2). An organisation may implement certain controls to protect the environment, however, those controls may not have considered the threats that could be introduced if these emerging technologies are adopted, further heightened by the interconnected ecosystem (Radanliev et al., 2020). All organisations must keep in mind that cyber is constantly evolving, and whenever something new is introduced from a technological perspective, it is key to understand the levels of comfort that there is no adverse risk introduced, the design of the technology and how it will play or interface with existing infrastructure is known (Part. 9). In an interconnected world, cybersecurity must be comprehensive, flexible, and collaborative. Cybercriminals have proved their capacity to take advantage of our online financial and market systems that are linked to the Internet. (Mohammed, 2015).

The cybersecurity posture was noted to be mature across the sector and linked to the way that risk is looked at overall within the organisations. Organisations have incorporated cybersecurity into the overall risk management framework of the organisations (Part. 4). Although, it was highlighted that changes in the technology inadvertently required changes in cybersecurity, highlighting the systems theory of the relationship between emerging technologies and cybersecurity (Wilkinson, 2011). Organisations depend severely on Information technology, and this is a critical factor of cybersecurity that requires adequate and effective processes. Other key attributes that were noted related to cyber posture were ensuring effective governance processes and transparency i.e., ensuring that senior management is kept abreast of

all the changes in the environment and also creating visibility for the board of directors (Part. 1), effective training and awareness programmes, ongoing monitoring, and alerts, testing, incident response, etc. (Part. 2). This is further influence by the use of emerging technologies (Mohammed, 2015). Raising awareness of cybersecurity issues and enhancing digital skills and abilities in terms of threat detection and management is regarded as a high-priority measure (Cirnu et al., 2018). People are often considered the weakest link in environments or computer networks and organisations are only as strong as their weakest link therefore training and awareness efforts are integral (Hatzivasilis et al., 2020).

Cyber hygiene practices were also noted as important aspects to ensure good cyber posture. Many organisations experience cyber breaches or have exposure to cyber threats because of poor cyber hygiene which is the minimum requirement from a cybersecurity perspective. According to Maennel et al. (2018), cybercrime is on the rise, and it is often assumed that proper cyber hygiene is required to secure digital networks and technology. The maturity is often disparate with varying degrees of maturity related to specific technologies and the level of adoption such as still being rated as immature from a cloud technology perspective due to the adoption of cloud within some organisations not necessarily as fast as others; and also, still maturing from an overall emerging technology perspective (Maennel et al., 2018).

Independent internal and external assessments as well as self-assessments were noted to be a common practice across the sector to understand the cybersecurity posture (Part. 3). Cybersecurity is noted as very important and most organisations have a very good track record for cybersecurity, in terms of keeping systems safe and secure. The key is to identify the relationship between emerging technologies and cybersecurity and the relevant requirements to ensure organisations are secure regardless of the technology that's adopted (Rodrigues et al., 2022).

Emerging technologies do expose the entities; it extends the digital footprint, and entities need to be wide awake to every setting and configuration. It was noted that Cyber security maturity was increasing, although some thought that they were not where they wanted to be and were very sceptical of ever saying that cyber was fully mature, so cybersecurity risks will always remain. According to Sarker et al. (2022), The key to offering a dynamically improved and up-to-date security system is to

leverage AI expertise, particularly machine and deep learning solutions (Sarker et al., 2022).

5.3.1 *Sub-theme: Cybersecurity risk and vulnerability management*

This sub-theme is linked to theme 2 and answers the sub-question; trying to determine the risk management processes that organisations have to implement or update due to changes in emerging technologies.

The implementation of effective controls and effective process adoption leads to structured identification, protection, detection, response and recovery processes within the organisations. These are key high-level requirements that are often non-negotiable when discussing cyber posture or maturity and that are related to the organisation's ability to identify its business-critical assets and systems to manage cyber risks. These are the organisation's ability to protect those business-critical assets, detect any cybersecurity incidents, be able to respond to those incidents, and the ability to recover its systems or services that were impacted by the incidents (Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, 2018).

The proliferation of digital has given rise to cyber scams such as extortion, denial of service attacks, and fraud. The frequency of cyber incidents is steadily increasing. To reduce these occurrences, it is critical to first identify what cyber threats to the organisations are (Kaur et al., 2021). Cyber security measures or controls need to be in place and assessed each time new technologies are adopted or if there are major changes to reduce the risk of exposure due to vulnerabilities either in the environment or introduced to the adoption of new or emerging technologies, due to the adverse impact of emerging technologies on cybersecurity (Corallo et al., 2020). Creating discipline and understanding with clear visibility across the organisation is imperative in every organisation. It is critical for organisations to also develop the discipline and awareness of what the technical resources are capable of so that risks can be effectively managed (Part. 1). Third-party risk is one of the issues that have emerged that has a major impact from a cyber perspective, organisations can exert control over their internal operations, however, it's difficult to exert such control over external entities with threat actors aware of this, resulting in supply chain assaults as well as data exfiltration through third parties (Part. 4). Cyber risk is heightened from a third -

party perspective and therefore robust processes must be in place to understand the technology, the risk introduced, the level of support provided from the service provider, etc. before the technology being implemented in the environment (Part. 10). Cybersecurity is key in the protection of organisations assets to halt cyber-attacks or cybercrime. According to Rodrigues et al. (2022), vulnerabilities exposed are usually attributed to bad decisions made in the adoption of new technologies (Rodrigues et al., 2022).

The organisations were noted to have a Security Operations Centre (SOC) environment, either physical or virtual, for the ongoing monitoring of the organisation's systems and networks, with the use of various common tools for logging monitoring and logging of events or incidents. Vielberth et al. (2020) noted that the significance of the SOC has expanded substantially, particularly in the last five years. This is mostly due to the critical need of preventing significant cyber catastrophes and the subsequent adoption of centralised security operations in the organisation. Many incidents or attacks go undetected in the environment, and the SOC allows for more effective detection capabilities (Vielberth et al., 2020).

5.4 Theme 3: Impact of emerging technologies on Cybersecurity

This theme is linked to the main question and trying to determine if the adoption or implementation of emerging technologies has an impact on cybersecurity and what that impact IS.

The threat landscape as well as the attack surface is continually changing. Organisations are continually under attack, and hackers continually trying to attack. Threat actors getting smarter with more opportunities created due to the advent of new and emerging technologies like AI, ML and the growth of cloud technologies (Part. 2). This has significant implications for cyber-security, given the rise in sophistication in cyber-attack landscapes as a result AI-based cyber-attacks. According to Ukwandu et al. (2021), Cybercriminals have used recent breakthroughs in AI to automate attack procedures by taking advantage of technologically increased learning and automation capabilities provided by machine learning (Ukwandu et al., 2021). By exploiting the weaknesses introduced by implementing emerging technologies such as AI and cloud

computing, a rising number of cybersecurity breaches hurt organisations. Cyber-attacks on the key infrastructure of businesses have the potential to destroy organisations. Knowing and evaluating the most critical assets to be safeguarded from future cyber-attacks and the business repercussions that may occur in advance is key to ensuring the safety and soundness of the entity and sector at large (Corallo et al., 2020).

Businesses may not be fully ready or aware of the risks introduced by emerging technologies leading to cyber-attacks and breaches (Cirnu et al., 2018). These attacks have the potential to disrupt infrastructure and, in the worst-case scenario, jeopardise the entire system, one key root cause would be by granting unauthorised users access. The impact, however, is disparate, and entities may find that when extending the control environment based on the possible risks introduced by emerging technologies could result in a continuously expanding process, requiring additional controls on an ongoing basis (Radanliev et al., 2020).

Many organisations look to grow their businesses, by identifying new markets and segments, and this is often done through identifying emerging technologies and digital strategies as a means to achieve their objectives. This, however, could have significant consequences and the view was to get businesses not to fall for shiny objects and to think about what value the technology provides and what the risk is of adopting the emerging technologies (Part.1). These new technologies could potentially introduce new entry points for attacks so entities will need to understand what should be done. This could be in multiple forms including new malware created considerably faster than in the past, due to the capabilities of machine learning algorithms and massive language models to generate code. Organisations have to be continuously aware of their environment and anticipate any change (Part. 4). Cybersecurity should be integral in any organisation and organisations should ensure that it’s incorporated into the overall Organisational and Information technology strategy (Corallo et al., 2020).

The discussions highlighted that the impact is not necessarily all negative and can be used positively and in defensive strategies to counter the attack. Various key activities could be developed such as Big data and machine learning capabilities that could allow capabilities of able to detect any anomalies better; AI that focuses on behavioural

analysis could be incorporated in systems to identify anomalies of potentially suspicious behaviour; machine learning could reduce false positives tremendously to prevent alert fatigue; the ability to anticipate new malware to be produced much quicker than previously done from a cyber perspective; large language models developed to assist with phishing, specifically with the ability of machine learning algorithms and large language models to write code, etc. There are numerous opportunities for organisations. Big data and machine learning capabilities can create the possibility to improve the ability to detect anomalies as well as other AI-powered solutions that focus on behavioural analysis, detecting anomalies of possibly suspicious behaviour (Part.1).

The impact of emerging technologies on cybersecurity can be catastrophic, with AI and ML already featuring prominently in key activities in the financial sector and cloud computing being adopted and a whirlwind pace. This in itself is a major factor in the evolution of cybercrime and the growth of cybersecurity, creating and exposing multiple gaps and vulnerabilities in organisations' technological environments (Rodrigues et al., 2022b).

5.4.1 *Sub-theme: Ability to adapt and respond*

This is a sub-theme of theme 3 and is linked to the sub-question, trying to determine if organisations can adequately adapt and respond to any cybersecurity attacks or breaches as a result of emerging technologies in cybersecurity.

The deployment of relevant tools and capabilities so that organisations can adapt and respond adequately and effectively. Entities must have documented response processes and procedures to manage the change in the landscape. The emergence of platforms is the future in cybersecurity which is utilised for various key aspects including to determine if the tooling or technologies are outdated and if a refresh is required. Proactive risk assessments are conducted to see if organisations can respond based on the current control environment or whether, with the new technologies, new security measures have to be implemented (Part. 4). According to Cirnu et al. (2018) it's vital to maintain the integrity, reliability and confidentiality of

organisations systems to always ensure the organisation is protected against malicious activities and minimises exposure (Cirnu et al., 2018).

There are often challenges experienced with adapting and responding where new or emerging technologies are implemented as the dynamic nature of the technology makes it difficult to follow set standards and processes (Part. 1). However, it was noted that organisations must implement processes to allow them to adapt and respond appropriately. Hatzivasilis et al. (2020) noted that systems are continuously under attack, with hackers trying to expose vulnerabilities or exploit any weakness that exists in the environment (Hatzivasilis et al., 2020). It was, however, discussed that organisations within the financial sector have a very mature response and detection capability, with 24/7 monitoring and alerting in most cases that create alerts (Part 11).

5.5 Summary of Analysis

The results are depicted in Chapter 4 and categorised into themes that were the basis for Chapter 5. In Chapter 5, the three themes and three sub-themes that were identified in Chapter 4 were analysed. The adoption of emerging technologies by financial institutions was highlighted, together with the overall cyber risk management processes and the cyber control environment, and the ultimate impact that emerging technologies has on cybersecurity. The adoption of technologies such as AI and ML are noted along with the influence it has on cybersecurity. The elements of this chapter lead into the concluding chapter to follow.

CHAPTER 6. CONCLUSION AND RECOMMENDATIONS

6.1 Introduction

The Chapter concludes the research study by reaffirming the views obtained from the results of the study. The findings of the study have been presented and the researcher, after examining the main findings, provides a view of the main aspects of the study that's linked to the overall objectives. The researcher also provides a brief view of the limitations of the study before providing some recommendations based on the study.

The purpose of the research was to determine the perceived impact of emerging technologies. i.e., technologies such as AI, ML and cloud computing on Cybersecurity in the South African Financial sector. Information Technology Risk and Cybersecurity experts were selected based on their holistic knowledge and experience in the field.

The research objectives are depicted below:

- Determine the impact of emerging technologies on the cybersecurity posture of financial institutions in South Africa.
- Determine the relationship between emerging technologies and cybersecurity and how emerging technologies influence cybersecurity.

The overall impact and influence were analysed and understood according to the System Theory, where various factors and dynamics were considered. The study delved deeper into the determination based on the lack of pertinent information, with the study aimed specifically at the financial sector in South Africa, including banks, insurers and market infrastructures. By considering these elements within a theoretical framework, the researcher was able to understand the complex relationship between emerging technologies and cybersecurity. According to the system theory, there was a relationship found between the adoption of emerging technologies and the influence on cybersecurity, with the need to review the cybersecurity control environment each time emerging technologies are adopted (Cirnu et al., 2018).

The thematic analysis was adopted according to the six-step process as highlighted by Braun and Clark, (2006) which allowed for a holistic analysis of the data collected

through semi-structured interviews (Braun & Clark, 2006b). This allowed for the three themes listed below to emerge from the data to confirm the impact that emerging technologies have on cybersecurity and to highlight how these technologies influence the cybersecurity control environments of organisations and the sector at large.

- **Theme 1:** Emerging Technologies and their Adoption - newer or unknown technologies, adopted at various levels and speeds within the organisations.
- **Theme 2:** Cybersecurity Posture and Controls - the cybersecurity maturity within the organisation and the types of controls implemented.
- **Theme 3:** Impact of emerging technologies on cybersecurity - the result of implementing new technologies and the effect it has on the cybersecurity control environment of the organisation.

6.2 Conclusion of the research study

The inspiration for the course of study was based on the view that emerging technologies had a huge impact on cybersecurity in South Africa, similar to the rest of the world. Furthermore, there was a relationship between adopting emerging technologies and the changes required in cybersecurity. Financial institutions in South Africa are known to be adopting new and emerging technologies such as AI, ML and cloud computing at a rapid pace (Gong & Ribiere, 2021). This is incorporated into the technology and digital strategies of the organisations and closely linked to the overall business strategies.

Many researchers believe emerging technologies to be the key attribute required to take organisations to the next level, creating a multitude of different business opportunities. However, most researchers in the field of cybersecurity believe that adopting new and emerging technologies without simultaneously considering the cybersecurity control environment of organisations would lead to major financial and non-financial losses. This emphasises the Systems Theory of the relationship between emerging technologies and cybersecurity.

The study highlighted, that emerging technologies such as artificial intelligence, machine learning, and cloud computing provide new opportunities for organisations but also create major problems in the cybersecurity landscape. The adoption of new

unknown technologies is a critical factor in the growth of the cyber threat landscape (Hatzivasilis et al., 2020). The study emphasised that strategies for risk management should be evaluated in the context of new technology adoption and further highlighted that people play an important role in cybersecurity. i.e., either as potential threats or as defenders.

This research, therefore, highlighted that financial institutions in South Africa are adopting technologies at a rapid pace regardless of the nature of the financial entity. The technology has been proven to have the capabilities to provide a plethora of alternative opportunities to either expand with existing products, providing better more efficient processes and services or expanding into different areas with different products, quicker, with limited experience.

This research, however, confirmed that the adoption of emerging technologies by financial institutions in South Africa does have a major impact on cybersecurity. However, there are both positive and negative connotations to the overall impact, although is largely linked to the attack and defence strategies of cybersecurity. The impact could result in the introduction of many unknown cyber risks into the organisation and sector, creating multiple vulnerabilities that could leave the organisation exposed to cyber-attacks and possibly leading to systemic risk in the sector, or the impact could result in the use of emerging technologies to better identify the vulnerabilities introduced and mitigate the risk (Participants).

6.3 Summary of Findings

The findings in Chapter 4 explore the adoption of emerging technologies including digital technologies, the cybersecurity maturity of organisations and the adverse impact that the technologies have on cybersecurity.

6.3.1 *Emerging Technologies and their Adoption Limitations*

To ascertain the level of understanding in terms of emerging technologies including digital technologies that are being adopted and the rate at which it’s adopted within the organisations.

- The consensus across the sector was that technology is ever-evolving.
- The data highlighted that most participants referred to emerging technologies as AI, ML and cloud computing, although some participants felt that the cloud was no longer emerging.
- The adoption was noted to be fairly aggressive across the sector.
- Digital transformation strategies were noted to be strongly linked to emerging technologies with a large spectrum of the sector adopting digital technologies or moving towards being more digitally run businesses.

6.3.2 *Cybersecurity Posture and Controls*

To identify the cybersecurity maturity within the organisation and the types of controls implemented before and after the adoption of emerging technologies.

- The cyber posture across the sector was noted to be fairly mature.
- A mature cyber posture was regarded as one of the most important aspects of the business and in most cases, driven from the top.
- Ongoing assessment and assurance of controls to test adequacy and effectiveness were noted as imperative.
- An effective risk and vulnerability management process is key.
- Building overall resilience and establishing effective incident response capabilities were noted as key components of cybersecurity, given the interrelated nature of emerging technologies and their impact on cybersecurity.

6.3.3 *Impact of emerging technologies on cybersecurity*

To determine the result of implementing new technologies and the effect it has on the cybersecurity control environment of the organisation and the sector.

- The consensus throughout the data suggested that all the aforementioned emerging technologies had a major impact on cybersecurity, requiring organisations to always factor cybersecurity into their technology adoption discussions.

- The data highlighted that some felt that there were major opportunities presented by emerging technologies for the improvement of the cybersecurity posture and control environment.
- Organisations can never fully view themselves as safe and secure and have to continually monitor their control environment.
- The control environment is expected to become ineffective with the emergence of new technologies and digitisation, rendering certain controls worthless and redundant.
- Cybersecurity practices are not cast in stone and there is a need for them to be adaptable and to be able to be moulded to manage any sort of identified emerging threats introduced by new or emerging technologies.

6.4 Limitations

The limitations were related to the research instrument utilised to conduct data collection and the timeframe. The semi-structured interviews were conducted disparately over a longer period as availability was a problem in some cases. The study was limited to entities from Johannesburg and Pretoria in Gauteng and Stellenbosch in the Cape provinces. The research sample consisted of three industries: banks, insurers and market infrastructures from the financial sector. The technologies were limited to the widely known technologies i.e., AI, ML and cloud computing, and although other technologies such as IoT, Quantum computing and crypto were touched on, it was not considered as a key determiner for this study.

6.5 Recommendations

The research study allowed for the gathering of a wealth of information, a lot of the information was sensitive, however, there was also a plethora of non-sensitive information that may not be generally known across the sector and could be beneficial to maintain the safety and soundness of the sector. This would be possible if the information is shared across the sector. Information that could help improve the cybersecurity posture of organisations and create awareness around various threats that may exist with possible mitigations. Existing industry and sector bodies or committees should be used within the sector to set up information-sharing knowledge

platforms. This could include the use of existing industry bodies or the creation of new bodies with specific mandates linked to the sharing of information. There could also be sharing mechanisms on a social medium for less sensitive data and on more formal platforms for sensitive type data. The processes of how to deal with certain threats may be less sensitive in nature, however, more beneficial to the sector and easier to share through social platforms. Events, incidents or breaches with more sensitive type information where the entity is known, or there was a loss of money or data could be shared or more formalised tools where access is restricted.

The study looked at systems theory as the theoretical framework to explore the impact of emerging technologies on cybersecurity, future studies could employ a combination of Roger's Diffusion of innovation theory and the General Systems theory which are not directly linked, however, could be adopted in a way that complements each other in further studies on emerging technologies and its impact on cybersecurity. This study could delve deeper into the specific relationship between emerging technologies and specific cybersecurity threats, whether certain threats are more influenced than others.

6.6 Suggestions for further research

The objective of this research study was to determine the perceived impact of emerging technologies on cybersecurity in banks, insurers and market infrastructures within the South African financial sector.

- Additional research can be conducted with a wider focus on the entire South African financial sector, including industries like medical aids, pension funds, investment houses, etc.
- The technology spectrum could be expanded to include other technologies such as Quantum computing, IoT, Crypto assets, Nanotechnology, Virtual and Augmented reality, etc.

The data collection methodology should not be limited to semi-structured interviews and should include surveys or questionnaires, perhaps using a mixed-method research approach. Greater methods to test the representation and credibility of the data should be applied (Cutcliffe & McKenna, 1999).

REFERENCES

Akter, S., Michael, K., Uddin, M. R., McCarthy, G., & Rahman, M. (2020). Transforming business using digital innovations: the application of AI, blockchain, cloud and data analytics. Annals of Operations Research, 308(1–2), 7–39. https://doi.org/10.1007/s10479-020-03620-w

Anfara, V. A., Jr, & Mertz, N. T. (2014). Theoretical Frameworks in Qualitative Research. SAGE Publications.

Arbel, L. (2015). Data loss prevention: the business case. Computer Fraud &Amp; Security, 2015(5), 13–16. https://doi.org/10.1016/s1361-3723(15)30037-3

Arnold, D. (2013). Traditions of Systems Theory: Major Figures and Contemporary Developments. Routledge.

Baur-Yazbeck, S., Frickenstein, J., & Medine, D. (2019). CYBER SECURITY IN FINANCIAL SECTOR DEVELOPMENT. Federal Ministry for Economic Co-operation and Development. https://www.findevgateway.org/sites/default/files/publications/files/cyber_security_paper_november2019.pdf

BCG Global. (2022). Digital Transformation. https://www.bcg.com/capabilities/digital-technology-data/digital-transformation/overview?utm_source=search&utm_medium=cpc&utm_campaign=digital&utm_description=none&utm_topic=digital_transformation&utm_geo=global&utm_content=digital_transformation_general&gclid=Cj0KCQjw2

MWVBhCQARIsAIjbwoPaEbz6ui8QJMuUxOlo6_oQYtQUDPW56COdVJC7I-osDWIUEn8mTpYaAhzKEALw_wcB

Braun, V., & Clarke, V. (2006a). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Braun, V., & Clarke, V. (2006b). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Byrne, M. D. (2021). Cybersecurity and the New Age of Ransomware Attacks. Journal of PeriAnesthesia Nursing, 36(5), 594–596. https://doi.org/10.1016/j.jopan.2021.07.004

Caldwell, T. (2011). Data loss prevention – not yet a cure. Computer Fraud &Amp; Security, 2011(9), 5–9. https://doi.org/10.1016/s1361-3723(11)70089-6

Chatfield, A. T., & Reddick, C. G. (2019). A framework for Internet of Things-enabled smart government: A case of IoT cybersecurity policies and use cases in U.S. federal government. Government Information Quarterly, 36(2), 346–357. https://doi.org/10.1016/j.giq.2018.09.007

Cirnu, C. E., Rotună, C. I., Vevera, A. V., & Boncea, R. (2018). Measures to Mitigate Cybersecurity Risks and Vulnerabilities in Service-Oriented Architecture. Studies in Informatics and Control, 27(3), 359–368. https://doi.org/10.24846/v27i3y201811

Computers & Security - Journal - Elsevier. (n.d.). Retrieved November 5, 2022, from https://www.journals.elsevier.com/computers-and-security

Corallo, A., Lazoi, M., & Lezzi, M. (2020). Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts. Computers in Industry, 114, 103165. https://doi.org/10.1016/j.compind.2019.103165

Creswell, J. W. (1998). Qualitative Inquiry and Research Design: Choosing Among Five Traditions. SAGE Publications, Incorporated.

CrowdStrike. (2022, March 30). What is Data Loss Prevention (DLP)? [Beginners Guide] | CrowdStrike. crowdstrike.com. https://www.crowdstrike.com/cybersecurity-101/data-loss-prevention-dlp/

Cutcliffe, J. R., & McKenna, H. (1999). Establishing the credibility of qualitative research findings: the plot thickens. Journal of Advanced Nursing, 30(2), 374–380. https://doi.org/10.1046/j.1365-2648.1999.01090.x

De Lanerolle, I. (2016, June 6). Internet freedom: Why access is becoming a human right. The Media Online. Retrieved November 8, 2022, from http://themediaonline.co.za/2016/06/internet-freedom-why-access-is-becoming-a-human-right/

DeJonckheere, M., & Vaughn, L. M. (2019). Semistructured interviewing in primary care research: a balance of relationship and rigour. Family Medicine and Community Health, 7(2), e000057. https://doi.org/10.1136/fmch-2018-000057

Deloitte. (2018). Managing Risk in Digital Transformation. https://www2.deloitte.com/content/dam/Deloitte/za/Documents/risk/za_managing_risk_in_digital_transformation_112018.pdf

Deloitte. (2020, April 24). Disruptive digital technologies in the financial services industry. https://www2.deloitte.com/us/en/pages/financial-services/articles/disruptive-digital-technologies-in-the-financial-services-industry.html

Dimitrov, W. (2020). The Impact of the Advanced Technologies over the Cyber Attacks Surface. Advances in Intelligent Systems and Computing, 509–518. https://doi.org/10.1007/978-3-030-51971-1_42

European Systemic Risk Board (ESRB). (2020). Systemic cyber risk. https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf

Fernandez De Arroyabe, I., Arranz, C. F., Arroyabe, M. F., & Fernandez De Arroyabe, J. C. (2023). Cybersecurity capabilities and cyber-attacks as drivers of investment in cybersecurity systems: A UK survey for 2018 and 2019. Computers &Amp; Security, 124, 102954. https://doi.org/10.1016/j.cose.2022.102954

Forbes. (2019, July 30). The Fintech Revolution: Who Are The New Competitors In Banking? https://www.forbes.com/sites/esade/2019/07/30/the-fintech-revolution-who-are-the-new-competitors-in-banking/?sh=59d175ae1161

Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. (2018). https://doi.org/10.6028/nist.cswp.04162018

Gartner. (2022). What Is Cybersecurity? https://www.gartner.com/en/topics/cybersecurity#:%7E:text=Cybersecurity%20is%20the%20practice%20of,sensitive%20information%20from%20digital%20attacks.

Gcaza, N., & Von Solms, R. (2017). A Strategy for a Cybersecurity Culture: A South African Perspective. The Electronic Journal of Information Systems in Developing Countries, 80(1), 1–17. https://doi.org/10.1002/j.1681-4835.2017.tb00590.x

Glossary. (n.d.). National Initiative for Cybersecurity Careers and Studies. Retrieved November 6, 2022, from https://niccs.cisa.gov/cybersecurity-career-resources/glossary

Gong, C., & Ribiere, V. (2021). Developing a unified definition of digital transformation. Technovation, 102, 102217. https://doi.org/10.1016/j.technovation.2020.102217

Grahn, S., Granlund, A., & Lindhult, E. (2021). Barriers to Value Specification when Carrying out Digitalization Projects. Technology Innovation Management Review, 11(5), 54–64. https://doi.org/10.22215/timreview/1442

Griffiths, J. (2017). Cyber security as an emerging challenge to South African national security. University of Pretoria. https://repository.up.ac.za/handle/2263/62639

Guggenmos, F., Häckel, B., Ollig, P., & Stahl, B. (2022). Security First, Security by Design, or Security Pragmatism – Strategic Roles of IT Security in

Digitalization Projects. Computers &Amp; Security, 118, 102747. https://doi.org/10.1016/j.cose.2022.102747

Haidros, H., Manzil, R., & Naik, M. (2021). An Overview on Cyber Attacks : Impacts and Mitigations. In Data Mining & Predictive Analytics. Today & Tomorrow's Printers and Publishers, New Delhi – 110002. https://www.researchgate.net/publication/365244274_An_Overview_on_Cyber_Attacks_Impacts_and_Mitigations

Hatzivasilis, G., Ioannidis, S., Smyrlis, M., Spanoudakis, G., Frati, F., Goeke, L., Hildebrandt, T., Tsakirakis, G., Oikonomou, F., Leftheriotis, G., & Koshutanski, H. (2020). Modern Aspects of Cyber-Security Training and Continuous Adaptation of Programmes to Trainees. Applied Sciences, 10(16), 5702. https://doi.org/10.3390/app10165702

Higgs, G., Price, A., & Langford, M. (2022). Investigating the impact of bank branch closures on access to financial services in the early stages of the COVID-19 pandemic. Journal of Rural Studies, 95, 1–14. https://doi.org/10.1016/j.jrurstud.2022.07.012

Hougaard, C. (2022, June 9). Financial sector innovation and cybersecurity risks. Cenfri. https://cenfri.org/publications/financial-sector-innovation-and-cybersecurity-risks/

Investopedia. (2021, February 23). Financial Services Sector. https://www.investopedia.com/ask/answers/030315/what-financial-services-sector.asp

Karjalainen, M., Sarker, S., & Siponen, M. (2019). Toward a Theory of Information Systems Security Behaviors of Organizational Employees: A Dialectical Process Perspective. Information Systems Research, 30(2), 687–704. https://doi.org/10.1287/isre.2018.0827

Kaur, G., Lashkari, Z. H., & Lashkari, A. H. (2021). Cybersecurity Threats in FinTech. In Springer eBooks (pp. 65–87). https://doi.org/10.1007/978-3-030-79915-1_4

Kothari, C. R. (2013). Research Methodology: Methods and Techniques (English, Spanish, French, Italian, German, Japanese, Chinese, Hindi and Korean Edition) (2nd ed.). New Age International Pvt Ltd Publishers. https://books.google.co.za/books?hl=en&lr=&id=hZ9wSHysQDYC&oi=fnd&pg=PA2&dq=a+research+APPROACH++is+defined+as&ots=1tYdpFf4E5&sig=OXWJZmlXzR02QWW72oh35AD8dKQ#v=onepage&q=a%20research%20APPROACH%20%20is%20defined%20as&f=false

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

Lee, I. (2017). Big data: Dimensions, evolution, impacts, and challenges. Business Horizons, 60(3), 293–303. https://doi.org/10.1016/j.bushor.2017.01.004

Lezzi, M., Lazoi, M., & Corallo, A. (2018). Cybersecurity for Industry 4.0 in the current literature: A reference framework. Computers in Industry, 103, 97–110. https://doi.org/10.1016/j.compind.2018.09.004

Li, H., Yoo, S., & Kettinger, W. J. (2021). The Roles of IT Strategies and Security Investments in Reducing Organizational Security Breaches. Journal of Management Information Systems, 38(1), 222–245. https://doi.org/10.1080/07421222.2021.1870390

Liquid Tech. (2021). The evolving Cyber Security threat in Africa. https://liquid.tech/wps/wcm/connect/corp/00d614b5-e6cf-4552-9085-c12e47b6246c/Liquid+Intelligent+Technologies+Cyber+security+Report+2021.pdf?MOD=AJPERES&CVID=nKxjVS0

Lucas, H. C., & Goh, J. M. (2009). Disruptive technology: How Kodak missed the digital photography revolution. The Journal of Strategic Information Systems, 18(1), 46–55. https://doi.org/10.1016/j.jsis.2009.01.002

Lyu, W., & Liu, J. (2021). Artificial Intelligence and emerging digital technologies in the energy sector. Applied Energy, 303, 117615. https://doi.org/10.1016/j.apenergy.2021.117615

Macas, M., Wu, C., & Fuertes, W. (2022a). A survey on deep learning for cybersecurity: Progress, challenges, and opportunities. Computer Networks, 212, 109032. https://doi.org/10.1016/j.comnet.2022.109032

Macas, M., Wu, C., & Fuertes, W. (2022b). A survey on deep learning for cybersecurity: Progress, challenges, and opportunities. Computer Networks, 212, 109032. https://doi.org/10.1016/j.comnet.2022.109032

Maennel, K., Mäses, S., & Maennel, O. (2018). Cyber Hygiene: The Big Picture. In Lecture Notes in Computer Science (pp. 291–305). Springer Science+Business Media. https://doi.org/10.1007/978-3-030-03638-6_18

Malatji, M., Von Solms, S., & Marnewick, A. (2019). Socio-technical systems cybersecurity framework. Information and Computer Security, Vol. 27 No. 2, Pp. 233-272., 27(2), 233–272. https://doi.org/10.1108/ics-03-2018-0031

Maleh, Y. (2021). Digital Transformation and Cybersecurity in the Context of COVID-19 Proliferation. ResearchGate. https://www.researchgate.net/publication/354678049_Digital_Transformation_and_Cybersecurity_in_the_Context_of_COVID-19_Proliferation

MARS Technology. (2018, November 7). How Digital transformation will Impact Cybersecurity. Mars Technologies. https://marstechnology.net/how-digital-transformation-will-impact-cybersecurity/

McKenna, N. (2021, October 19). What is the Relationship Between Digital Transformation and Cyber Security? McKenna Consultants. https://www.mckennaconsultants.com/what-is-the-relationship-between-digital-transformation-and-cyber-security/

Medoh, C., & Telukdarie, A. (2022). The Future of Cybersecurity: A System Dynamics Approach. Procedia Computer Science, 200, 318–326. https://doi.org/10.1016/j.procs.2022.01.230

Miles, M. B., & Huberman, A. M. (1994). Qualitative Data Analysis: An Expanded Sourcebook. SAGE.

Minishi-Majanja, M. K., & Kiplang'at, J. (2013). The diffusion of innovations theory as a theoretical framework in Library and Information Science research. South African Journal of Libraries and Information Science, 71(3). https://doi.org/10.7553/71-3-586

Mishra, S. (2023). Exploring the Impact of AI-Based Cyber Security Financial Sector Management. Applied Sciences, 13(10), 5875. https://doi.org/10.3390/app13105875

Mittal, V. (2019, January). South Africa FinTech Landscape. Researchgate. Retrieved August 2, 2022, from https://www.researchgate.net/publication/330701590_South_Africa_FinTech_Landscape

Mohammed, D. (2015). Cybersecurity Compliance in the Financial Sector. The Journal of Internet Banking and Commerce, 20(1), 1–11. https://www.icommercecentral.com/open-access/cybersecurity-compliance-in-the-financial-sector.pdf

Naidoo, S. (2021, July 27). Transnet cyber attack confirmed: Port terminals division declares force majeure. Moneyweb. https://www.moneyweb.co.za/news/companies-and-deals/transnet-cyber-attack-confirmed-port-terminals-division-declares-force-majeure/

Nelson, N., & Madnick, S. (2017). Studying the tension between digital innovation and cybersecurity. Cybersecurity Interdisciplinary Systems Laboratory (CISL), 1–12.

Nguyen Duc, A., & Chirumamilla, A. (2019). Identifying Security Risks of Digital Transformation - An Engineering Perspective. Lecture Notes in Computer Science, 677–688. https://doi.org/10.1007/978-3-030-29374-1_55

OECD. (2012). The Role of the 2002 Security Guidelines: Towards Cybersecurity for an Open and Interconnected Economy. OECD Digital Economy Papers, 209, 1–14. https://doi.org/10.1787/5k8zq930xr5j-en

OECD. (2021). Artificial Intelligence, Machine Learning and Big Data in Finance. https://www.oecd.org/finance/financial-markets/Artificial-intelligence-machine-learning-big-data-in-finance.pdf

PANCHOLI, S., & STROBL, G. (2019). CATCH-22: DIGITAL TRANSFORMATION AND ITS IMPACT ON CYBERSECURITY. RSM network. https://www.rsm.global/ireland/sites/default/files/media/catch-22_digital_transformation_and_cybersecurity_final.pdf

Pereira, C. S., Durão, N., Moreira, F., & Veloso, B. (2022). The Importance of Digital Transformation in International Business. Sustainability, 14(2), 834. https://doi.org/10.3390/su14020834

PWC. (2021). Emerging Cyber Threats in the Manufacturing and Mining Sectors (No. 9). https://www.pwc.co.za/en/assets/pdf/threat-advisory-manufacturing-mining-sector.pdf

Radanliev, P., De Roure, D., Page, K. R., Nurse, J. R. C., Montalvo, R. M., Santos, O., Maddox, L. T., & Burnap, P. (2020). Cyber risk at the edge: current and future trends on cyber risk analytics and artificial intelligence in the industrial

internet of things and industry 4.0 supply chains. Cybersecurity, 3(1). https://doi.org/10.1186/s42400-020-00052-8

Research at Grass Roots: For the Social Sciences and Human Services Professions. (2005). Van Schaik Publishers.

Rodrigues, A. L. S., Ferreira, J. J., Teixeira, F. L., & Zopounidis, C. (2022). Artificial intelligence, digital transformation and cybersecurity in the banking sector: A multi-stakeholder cognition-driven framework. Research in International Business and Finance, 60, 101616. https://doi.org/10.1016/j.ribaf.2022.101616

Rogowski, W. (2013). The right approach to data loss prevention. Computer Fraud &Amp; Security, 2013(8), 5–7. https://doi.org/10.1016/s1361-3723(13)70070-8

Rosencrance, L. (2022, January 4). security posture. SearchSecurity. https://www.techtarget.com/searchsecurity/definition/security-posture#:%7E:text=Security%20posture%20refers%20to%20an,to%20ever%2Dchanging%20cyber%20threats.

Rotolo, D., Hicks, D., & Martin, B. R. (2015). What is an emerging technology? Research Policy, 44(10), 1827–1843. https://doi.org/10.1016/j.respol.2015.06.006

Sahrom Abu, M., Rahayu Selamat, S., Ariffin, A., & Yusof, R. (2018). Cyber Threat Intelligence – Issue and Challenges. Indonesian Journal of Electrical Engineering and Computer Science, 10(1), 371. https://doi.org/10.11591/ijeecs.v10.i1.pp371-379

Sarker, I. H., Khan, A., Abushark, Y. B., & Alsolami, F. (2022). Internet of Things (IoT) Security Intelligence: A Comprehensive Overview, Machine Learning Solutions and Research Directions. Mobile Networks and Applications. https://doi.org/10.1007/s11036-022-01937-3

Shaikh, F. A., & Siponen, M. (2023). Information security risk assessments following cybersecurity breaches: The mediating role of top management attention to cybersecurity. Computers &Amp; Security, 124, 102974. https://doi.org/10.1016/j.cose.2022.102974

Shao, X., Siponen, M., & Liu, F. (2020). Shall we follow? Impact of reputation concern on information security managers' investment decisions. Computers &Amp; Security, 97, 101961. https://doi.org/10.1016/j.cose.2020.101961

Sharma, S. (2021). Role of Artificial Intelligence in Cyber Security and Security Framework. In Role of AI in Cyber Security. https://doi.org/10.1002/9781119760429.ch3

Stăncioiu, A. (2017). THE FOURTH INDUSTRIAL REVOLUTION &qout;INDUSTRY 4.0" (No. 1). Academica Brâncuşi. https://www.utgjiu.ro/rev_mec/mecanica/pdf/2017-01/11_Alin%20ST%C4%82NCIOIU%20-%20THE%20FOURTH%20INDUSTRIAL%20REVOLUTION%20%E2%80%9EINDUSTRY%204.0%E2%80%9D.pdf

Stewart, B. G., Schatz, R., & Khare, A. (2016). Making Sense of Digital Disruption Using a Conceptual Two-Order Model. In Springer eBooks (pp. 3–21). https://doi.org/10.1007/978-3-319-44468-0_1

Stock, J. R., & Boyer, S. L. (2009). Developing a consensus definition of supply chain management: a qualitative study. International Journal of Physical Distribution &Amp; Logistics Management, 39(8), 690–711. https://doi.org/10.1108/09600030910996323

Ukwandu, E. A., Okafor, E. N. C., Ikerionwu, C., Olebara, C., & Ugwu, C. (2021, September 13). Cyber-Security in the Emerging World of ’Smart Everything’. https://arxiv.org/abs/2109.05821.

umsl.edu. (2022). POPULATIONS AND SAMPLING. POPULATIONS AND SAMPLING. https://www.umsl.edu/%7Elindquists/sample.html

Varga, S., Brynielsson, J., & Franke, U. (2021). Cyber-threat perception and risk management in the Swedish financial sector. Computers &Amp; Security, 105, 102239. https://doi.org/10.1016/j.cose.2021.102239

Vial, G. (2019). JOURNAL OF STRATEGIC INFORMATION SYSTEMS REVIEW. Understanding Digital Transformation: A Review and a Research Agenda, 1(1), 1–71.

Vielberth, M., Böhm, F., Fichtinger, I., & Pernul, G. (2020). Security Operations Center: A Systematic Study and Open Challenges. IEEE Access, 8, 227756–227779. https://doi.org/10.1109/access.2020.3045514

Wilkinson, L. S. (2011). Systems Theory. In Springer eBooks (pp. 1466–1468). https://doi.org/10.1007/978-0-387-79061-9_941

Winston & Strawn. (2022). What is the Definition of Emerging Technology? | Winston & Strawn Legal Glossary. https://www.winston.com/en/legal-glossary/emerging-technology.html

World Bank. (2022). Overview. https://www.worldbank.org/en/topic/financialsector/overview

World Economic Forum (WEF). (2016). Understanding Systemic Cyber Risk. https://www.zurich.com/-/media/project/zurich/dotcom/industry-knowledge/cyber-risk/docs/wef-report-understanding-systemic-cyber-risk-oct-2016.pdf?rev=aa0177a7c54140c0bd593b0e8f4b2c3f

World Economic Forum (WEF). (2022). Global Cybersecurity Outlook 2022. https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2022.pdf

Wu, D., Ren, A., Zhang, W., Fan, F., Liu, P., Fu, X., & Terpenny, J. (2018). Cybersecurity for digital manufacturing. Journal of Manufacturing Systems, 48, 3–12. https://doi.org/10.1016/j.jmsy.2018.03.006

Xu, D. (2010). Cloud Computing: An emerging technology. https://doi.org/10.1109/iccda.2010.5541105

Xu, M., David, J. M., & Kim, S. H. (2018). The Fourth Industrial Revolution: Opportunities and Challenges. International Journal of Financial Research, 9(2), 90. https://doi.org/10.5430/ijfr.v9n2p90

Y. Connolly, L., & Wall, D. S. (2019). The rise of crypto-ransomware in a changing cybercrime landscape: Taxonomising countermeasures. Computers &Amp; Security, 87, 101568. https://doi.org/10.1016/j.cose.2019.101568

Ying, M. (2010). Quantum computation, quantum theory and AI. Artificial Intelligence, 174(2), 162–176. https://doi.org/10.1016/j.artint.2009.11.009

Zurich. (2014, December 1). Interconnected-risks-in-a-digital-economy. Digital, Data & Cyber. Retrieved June 13, 2022, from https://www.zurich.com/en/knowledge/topics/digital-data-and-cyber/interconnected-risks-in-a-digital-economy

APPENDIX A



Interview Questionnaire (Online Interviews)

Explain reason for interview: Performing a study to determine "The perceived impact of emerging technologies on cybersecurity in the South African financial sector".

You are a selected participant based on your experience and exposure in the said fields.

Verbal Consent: Please answer by way of saying Yes or No if you consent to being part of this study?

The information obtained will be anonomised and the institution details will be kept confidential.

Questions:

- Within the context of your organisation, what is your understanding of **EMERGING TECHNOLOGIES**?
  - Is your organisation currently deploying emerging technologies?
    - If the answer is Yes:
      - What technologies is the organisation exposed to or plan to adopt?
      - What is the technologies used for?
    - If the answer is No:
      - What is the plan to adopt these emerging technologies?
- What is the overall Digital Transformation strategy of the organisation?
  - Are these aggressive strategies or are they just experimental at this stage?
  - Within the context of your organisation, what is your understanding of emerging technologies?
- What is the current **CYBERSECURITY** posture of the organisation?

- How does the organisation assess or determine the cybersecurity requirements for the adoption of these technologies?
- Are cybersecurity measures assessed each time new technologies are adopted or only initially?
- Are existing cybersecurity controls used or is new control requirements assessed?
- Is there a process for the identification and assessment of cybersecurity risks and the impact due to the emerging technologies?
    - What is the mitigating actions if cybersecurity risks are identified?
- Is there additional focus on the exposure of the impact of the emerging technologies on cybersecurity?
    - What is the process where vulnerabilities in the cybersecurity measures are identified?
- Can the institution adapt and respond to new cybersecurity risks introduced by the emerging technologies?
    - What is the process if deficiencies are identified?

Concluding questions

- How do you see Emerging technologies impacting cybersecurity?
    - What new security measures have been implemented due to emerging technologies?
- Do you think the organisation have adequate cybersecurity controls to mitigate against the threats introduced by emerging technologies?
    - What cybersecurity controls were ineffective of inadequate based on the adoption of emerging technologies?

APPENDIX B



Wits Business School University of the Witwatersrand

PARTICIPANT INFORMATION SHEET

Dear Sir / Madam,

My name is Denzil Phillips. I am a final year student at Wits Business School enrolled in the Master of Management in Digital Business programme under the supervision of Dr Kiru Pillay. In fulfillment of the requirements to complete the academic programme, I have undertaken a research project to investigating the perceived impact of emerging technologies on cybersecurity in the South African financial sector. The research project aims to determine the impact that emerging technologies such as Artificial Intelligence, Cloud computing, etc., has on cybersecurity posture of financial institutions.

As part of this project, I would like to invite you to take part in a virtual interview through the Microsoft Teams platform. You will be required to answer questions on emerging technologies and cybersecurity in your institutions and the interview will take 30 - 45 minutes. I would also like to record (audio) the interview with your permission. This recording will be stored securely on a OneDrive folder, and only I, Denzil Phillips will access this recording. It will be deleted after a period agreed by Wits Business School.

Participating in this research project will not incur any personal costs. You will not receive any direct benefits from participation, and there are no disadvantages or penalties if you do not choose to participate in the study. You may cancel at any time or not answer any questions if you wish not to. You also have the choice to withdraw from the study at any time. The interview will be confidential, and your name will not be revealed in the final report. The information you provide will be held securely and

not disclosed to anyone. I will use a pseudonym (false name) to represent your participation in my final research report.

If you have any questions about this research, please do not hesitate to contact me at the details listed below. This study will be written up as a research report and may be published online through the university library website.

If you have any concerns or complaints regarding the ethical procedures of this study, you are welcome to contact the University Human Research Ethics Committee (Non-Medical) telephonically at +27(0) 11 717 1408, or via email hrecnon-medical@wits.ac.za.

Yours sincerely,

D Phillips

Researcher: Denzil Phillips, Email: 2488813@students.wits.ac.za

Supervisor: Dr Kiru Pillay, Email: kiru2010@gmail.com

Annexure C



Wits Business School
University of the Witwatersrand

CONSENT FORM

Research working title: The Perceived Impact of Emerging Technologies on Cybersecurity in the South African financial sector.

Name of researcher: Denzil Phillips

I, ……..., agree to participate in this research project. The research has been explained to me, and I understand what my participation will involve. I agree to the following:

(Please indicate the relevant options below)

I agree that my participation will remain confidential	YES	NO
I agree that the researcher may use anonymous quotes or false names in his research report	YES	NO

I agree that the interview may be audio recorded	YES	NO
I agree that the information I provide may be used anonymously after this project has ended for academic purposes by other researchers, subject to their own ethics clearance being obtained.	YES	NO

…… (signature)

…… (name of participant)

…… (date)

…… (signature)

…… (researcher's name)

…… (date)

Thank you for your participation.

Annexure D

Ethical Clearance

Graduate School of Business Administration
University of the Witwatersrand, Johannesburg

Wits Business School Ethics Committee
Constituted under the University Human Research Ethics Committee (Non-Medical)

Ethics Clearance Certificate

Ethics protocol number: WBS/DB2488813/756

This certificate is only valid with a legitimate ethics protocol number and signed by the Researcher (below).

Project title	The perceived impact of emerging technologies on cybersecurity in the South African financial sector
Investigator / Researcher	Mr Denzil Phillips
Nature of Project	MM (Digital Business)
Decision of the Committee	Approved, provided stakeholders and participants are guaranteed confidentialty.
Issue Date of Certificate	2023-02-06
Expiry date	Date of submission of the project / research report
Chairperson	Dr Pius Oba ☎ +27 11 717 3976 +27 82 733 6587 pius.oba@wits.ac.za

Declaration by Researcher

One copy must be signed by the Researcher and returned to the Chairperson of the Wits Business School Ethics Committee.

I fully understand the conditions under which I am authorized to carry out the abovementioned research and I guarantee to ensure compliance with these conditions. Should any departure to be contemplated from the research procedure as approved I undertake to resubmit the protocol to the Committee.

DDPhillips — Signature

07/02/2023 — Date:

Annexure E

Approved Topic

UNIVERSITY OF THE WITWATERSRAND, JOHANNESBURG

Private Bag 3 Wits, 2050
Fax:
Tel:

Reference: Ms Jennifer Mgolodela
E-mail: jennifer.mgolodela@wits.ac.za

22 August 2022
Person No: 2488813
PAG

Mr DD Phillips
P.O.Box 2112
Mondeor
2110
South Africa

Dear Mr Denzil Phillips

Master of Management: Approval of Title

We have pleasure in advising that your proposal entitled *The perceived impact of emerging technologies on cybersecurity in the South African financial sector* has been approved. Please note that any amendments to this title have to be endorsed by the Faculty's higher degrees committee and formally approved.

Yours sincerely

Mrs Marike Bosman
Faculty Registrar
Faculty of Commerce, Law and Management

Annexure F

Checklist

UNIVERSITY OF THE WITWATERSRAND JOHANNESBURG

WITS FACULTY OF COMMERCE, LAW & MANAGEMENT

THESIS/DISSERTATION/RESEARCH REPORT – FIRST SUBMISSION CHECKLIST FORM *(for Examination)*

Name of Candidate:	**Denzil Phillips**	
Person/Student Number:	**2488813**	
Qualification:	**Master of Management in the field of Digital Business**	
Title:	**Mr**	
Supervisor(s):	**Dr Kiru Pillay**	
Contact Details:	**Cell number(s): 084 200 1038**	**Email: denzil.phillips@resbank.co.za**

FIRST SUBMISSION CHECKLIST *(for Examination)*

Student to send:	**Electronic copy of research** *(Hard copy may be required upon request from the examiner)* **** WBS students are required to submit in MS Word format. All other schools must submit in PDF format. ****	X
	Full Turn-it-in Report *(signed by Supervisor)* **** For WBS Masters – this report does not require the Supervisor's approval ****	X
	Confirmation of Ethics *(Clearance/Waiver certificate or declaration)*	X
	Overall Supervisor Evaluation form *(MBA candidates ONLY)*	N/A
Supervisor to send:	**University Clearance Certificate** *(Supervisor to complete and send directly to Faculty)*	X
	Supervisor's Report *(Supervisor to complete and send directly to Faculty)*	X
Faculty to check on:	Approved title and supervisor(s)	
	Approved examiners	
	Registration status *(students must be registered during the examination period)*	

Please send your research submission to the correct email:

- #Fac-MBAsubmissions@wits.ac.za – for **MBA (ARP)** research submissions
- Veli.Mongwe@wits.ac.za – for PhD and Full Research Masters students **belonging to WBS**
- #Fac-MMsubmissions@wits.ac.za – for MM research submissions **belonging to WBS and WSG**
- Nasreen.Abdulla@wits.ac.za – for PhD and Full Research Masters students **belonging to WSG**
- Tshepo.Mohlakoane@wits.ac.za – for all research types **belonging to Commerce and Law (SEF, SBS, SOA and SOL)**

Please Note:

- *Outstanding fees must be cleared to enable Awaiting Examiner's registration.*
- *Incomplete submissions will NOT be prioritised.*
- *There may be a delay in the examination process where the research has been accepted by Faculty without approved examiners.*
- *If you submit by end-February, you are more likely to graduate in July.*
- *While Faculty will do all that is possible to streamline the research examination process, graduation is NOT guaranteed for any student.*
- *WBS submissions must undergo internal academic quality checks before the exam process may begin.*

Annexure G

Turnitin

2488813_Research Report _ MMDB 2022 v0.11.docx

ORIGINALITY REPORT

3%	3%	1%	%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	wiredspace.wits.ac.za Internet Source	1%
2	www.mdpi.com Internet Source	<1%
3	repository.nwu.ac.za Internet Source	<1%
4	www.cliffsnotes.com Internet Source	<1%
5	Wenjing Lyu, Jin Liu. "Artificial Intelligence and emerging digital technologies in the energy sector", Applied Energy, 2021 Publication	<1%
6	ujcontent.uj.ac.za Internet Source	<1%

Exclude quotes	On	Exclude matches	< 50 words
Exclude bibliography	On		

2488813_Research Report _ MMDB 2022 v0.13.docx

ORIGINALITY REPORT

3%	3%	1%	%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	wiredspace.wits.ac.za Internet Source	2%
2	www.mdpi.com Internet Source	<1%
3	www.cliffsnotes.com Internet Source	<1%
4	Wenjing Lyu, Jin Liu. "Artificial Intelligence and emerging digital technologies in the energy sector", Applied Energy, 2021 Publication	<1%
5	scholar.sun.ac.za Internet Source	<1%
6	repository.nwu.ac.za Internet Source	<1%
7	ujcontent.uj.ac.za Internet Source	<1%

Exclude quotes	On	Exclude matches	< 50 words