

https://dspace.org/

Evaluating cybersecurity governance challenges in South African fintechs

Nhliziyo, Norman

2025
University of the Witwatersrand, Johannesburg
https://hdl.handle.net/10539/47809
Nhliziyo, Norman. (2025). Evaluating cybersecurity governance challenges in South African fintechs [Master`s dissertation, University of the Witwatersrand, Johannesburg]. WIReDSpace. https://hdl.handle.net/10539/47809

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





Evaluating cybersecurity governance challenges in South African fintechs

by

Norman Nhliziyo

Supervisor: Dr. Sylvester Horvey

Protocol number: WBS/BA2696297/409

February 2025

A research article submitted to the Faculty of Commerce, Law, and Management, University of the Witwatersrand, in partial fulfilment of the requirements for the degree of Master of Business Administration.

Abstract

This research paper examines the key drivers and challenges of cybersecurity governance within South African fintech companies. The study found that compliance and risk management are the primary drivers for cybersecurity governance in fintechs. Compliance is regarded as a core responsibility for cybersecurity personnel, with achieving compliance objectives being a critical success factor for operating in the payments industry. Additionally, cybersecurity governance is integrated into a broader risk management approach, as fintechs consider cybersecurity as critical to ensuring business continuity and safeguarding reputational risk.

However, the study also found several challenges in implementing cybersecurity governance within fintechs. These include financial constraints, a shortage of cybersecurity talent, low perceived value of cybersecurity, and a lack of alignment between the cybersecurity function and the broader business. The study recommends that fintechs address these challenges by enhancing executive oversight on the cybersecurity function, adopting quantitative risk analysis frameworks, leveraging technology more effectively, and distributing cybersecurity responsibilities across the organisation.

Keywords

Cybersecurity, Governance, Risk, Compliance, Fintech

Declaration

I declare that this research report is my own work except as indicated in the references and acknowledgements. It is submitted in partial fulfilment of the requirements for the degree of Master of Business Administration at the University of the Witwatersrand, Johannesburg. It has not been submitted before for any degree or examination in this or any other university.

Name: NORMAN NHLIZIYO

Signature: 

Date: 2025-06-03 **Signed at**: BRYANSTON, JOHANNESBURG

Dedication

Amai,

Rairo yenyu, rairo yaambuya ndakacherechedza — “ita shungu”

Acknowledgements

All glory and honour and thanks to Jesus Christ, my Lord, and my God. Through Him, all things were made.

I want to extend my appreciation to my supervisor, Dr. Sylvester Hovey; thank you for your guidance and patience.

I have had the fortune of receiving immeasurable support from colleagues, friends, and family. For this I am filled with gratitude. I also want to thank the participants who volunteered their time to contribute to this study — I hope that the insights will aid your endeavours.

Finally, to my wife and children. Chido, your unwavering love and support throughout this challenging journey have been my anchor. Thank you for holding down the fort; I am eternally grateful. Batter up! Thembi and Nzani, my pride and joy. I cherish all the memories we spent together “working” on this project. May you be inspired to do more and go further.

Table of contents

Abstract i

Keywords ii

Declaration iii

Dedication iv

Acknowledgements v

List of tables ix

List of figures x

List of acronyms xi

1. Chapter 1: Research introduction 1

1.1. Statement of purpose 1

1.2. Background to the study 1

1.3. Problem statement 2

1.4. Research objectives 2

1.5. Research questions 3

1.6. Rationale of the study 3

1.7. Delimitation of the study 3

1.8. Definition of keywords 4

1.9. Structure of the article 4

2. Chapter 2: Literature review 5

2.1. Introduction 5

2.2. Empirical literature review 5

2.2.1. Fintech overview 5

2.2.2. Cybersecurity risk and cybersecurity governance drivers and challenges 6

2.3. Analytical framework 9

2.3.1. Conceptual framework 9

2.4. Conclusion 9

3. Chapter 3: Research methodology 10
3.1. Introduction 10
3.2. Research approach and design 10
3.3. Research paradigm 10
3.4. Data collection methods 11
3.4.1. Population 11
3.4.2. Sample and sampling method 11
3.5. Research instrument 11
3.6. Data collection procedure 12
3.7. Data analysis strategies and interpretation 12
3.8. Limitations 12
3.9. Quality assurance 13
3.9.1. External validity 13
3.9.2. Internal validity 13
3.9.3. Reliability 13
3.10. Ethical assurance 13
4. Chapter 4: Presentation and analysis of results 15
4.1. Introduction 15
4.2. Description of the sample 15
4.2.1. Fintech type 16
4.2.2. Fintech size 16
4.2.3. Organisation of the cybersecurity function 17
4.2.4. Participant's role and cybersecurity experience 17
4.3. Presentation of the results 18
4.3.1. Drivers for cybersecurity governance 18
4.3.1.1. Theme 1: The primacy of compliance and regulation 18
4.3.1.2. Theme 2: Cybersecurity as part of enterprise risk management 19

4.3.1.3. Theme 3: Cybersecurity as a differentiator 20
4.3.2. Challenges in cybersecurity governance 20
4.3.2.1. Theme 1: Shortage of cybersecurity capacity and talent 20
4.3.2.2. Theme 2: Financial constraints 21
4.3.2.3. Theme 3: Low value perceptions and lack of alignment 21
4.3.2.4. Theme 5: Evolving threat landscape 23
4.4. Discussion 23
4.4.1. Drivers for cybersecurity governance 23
4.4.2. Challenges in cybersecurity governance 24
4.5. Conclusion 26
5. Chapter 5: Conclusion and recommendations 27
5.1. Introduction 27
5.2. Conclusion 27
5.3. Recommendations 27
5.4. Limitations and further research 29
References 30
Appendix A — Research instrument 43
Appendix B — Research participation consent form 45
Appendix C — Research submission checklist 46
Annexure A — Research approval 47
Annexure B — Ethics clearance certificate 48
Annexure C — Turnitin originality report 49

List of tables

Table 1.1 Definition of keywords 4

Table 3.1 Number of fintechs identified by different sources in grey literature 11

Table 4.1 Description of the study's participants 15

List of figures

Figure 2.1 Conceptual framework 9
Figure 3.1 Research framework 10
Figure 4.1 Participant's organisation fintech type (payments vs non-payments) 16
Figure 4.2 Number of companies by employees 17
Figure 4.3 Participant's roles within fintech 18

List of acronyms

AI	Artificial Intelligence
CIS	Center for Internet Security
COBIT	Control Objectives for Information and Related Technology
DFS	Digital Financial Services
GFC	Global Financial Crisis
GRC	Governance, Risk, and Compliance
IEC	International Electrotechnical Commission
ISO	International Organisation for Standardisation
IT	Information Technology
NIST	National Institute of Standards and Technology
PASA	Payments Association of South Africa
PCI DSS	Payment Card Industry Data Security Standard
POPIA	Protection of Personal Information Act
SABRIC	South African Banking Risk Information Centre
SARB	South African Reserve Bank

1. Chapter 1: Research introduction

1.1. Statement of purpose

This research paper aims to evaluate the drivers for, and challenges of cybersecurity governance among emerging South African fintech companies.

1.2. Background to the study

Cybersecurity refers to the people, processes, and technologies used to protect computer systems from threats that result in loss (Schiliro, 2022). Due to the increasing rate of high-impact cyber incidents, there has been a heightened global attention on the issues around cybersecurity. Examples of major incidents that had a global impact include the WannaCry ransomware attack that resulted in the shutting down of critical infrastructure in across 150 countries and the NotPetya malware that caused similar damage (Kao & Hsiao, 2018; Manuel & Thomas, 2020). The damage exacted by these two incidents highlight the importance of effectively managing cybersecurity risk.

Although unprecedented, the above incidents are not isolated; however, exact costs resulting from cybersecurity incidents are unknown. Estimates, whilst questionable, provide insights on the magnitude of the problem (Świątkowska, 2020). For example, Cybersecurity Ventures (2020), predicted these costs to exceed $10 trillion globally by 2025 — a three-fold increase from the preceding decade that is approximately 10% of the projected global GDP in that year (O'Neill, 2024). Regarding South Africa, this research found no reliable data on the total costs inflicted by cybersecurity breaches; however, the number of high-profile incidents between 2010 and 2020 has largely followed an upward trajectory (Pieterse, 2021). More worryingly, according to Kaspersky, a leading cybersecurity company, a lack of cybersecurity skills has left a staggering 87% of businesses in the country ill-equipped to deal with cyber threats (Kaspersky, 2023). These statistics highlight the increasing relevance of cybersecurity risks and their substantial negative impact on organisations of all types and sizes.

Among the organisations affected by cybersecurity risks are fintechs, which are particularly susceptible due to the inherently digital nature of their services (Arner et al., 2015; Freund & Jones, 2015). This vulnerability is amplified by the rapid growth of the African fintech sector, where revenues are projected to increase thirteen-fold between 2021 and 2030 (Goyal et al., 2023). This growth is likely to attract more threat actors because of the increased potential

reward. Along with Nigeria, Kenya, and Egypt, South Africa is positioned as one of the key markets where this growth will occur. The country already boasts a thriving fintech industry consisting of over 140 entities (approximately 20% of Africa's total), that are managing a portfolio of assets valued at $7.5 billion (Disrupt Africa, 2023; Fintech Times, 2022; Naspers, 2024). These include startups that raised over $700 million in funding between 2015 and 2023 (Disrupt Africa, 2023; Fintech Times, 2022). Fintechs, therefore, play a crucial role in society, providing essential services and creating jobs. Further, as South Africa pursues a cashless society and further integrates technology, their importance will only grow (South African Reserve Bank, 2024). Therefore, understanding and addressing the cybersecurity risks facing fintechs is paramount.

1.3. Problem statement

According to the World Economic Forum (2023), cybersecurity risk is the most significant technological risk and ranks among the top ten short- and medium-term risks for organisations worldwide. For fintechs, the realisation of this risk can significantly disrupt financial health, market standing, operational efficiency, legal compliance, and reputation (Goh et al., 2020). In addition, due to the interconnectedness within the financial services industry and the increasing digital dependency of consumers, the impact of cybersecurity extends beyond the targeted fintech, affecting other parties as well (Goh et al., 2020). Consequently, effective cybersecurity governance is considered a critical success factor for fostering sustainable fintech ecosystems (Ehrentraud & Ocampo, 2020; Werth et al., 2023). However, for this governance to be truly effective, it is necessary to understand its drivers and the challenges that hinder its implementation.

Within the South African context, cybersecurity challenges are widely acknowledged at both national and industry levels (Griffiths, 2016; Sutherland, 2017); however, the specific vulnerabilities, threats, and mitigation strategies relevant to fintechs in South Africa have not been fully researched. Despite the growing body of literature on cybersecurity in broader financial and industrial contexts, no comprehensive study has systematically examined the specific cybersecurity landscape for fintechs in South Africa. Addressing this gap is crucial to ensuring the long-term stability and trustworthiness of fintech ecosystems in the country.

1.4. Research objectives

The following are the research objectives (ROs) of the study:

- **RO1:** Identify the main drivers for cybersecurity governance in fintechs.
- **RO2:** Identify the challenges in implementing cybersecurity programmes in fintechs.

1.5. Research questions

Based on the above objectives, the research questions (RQs) that the study will answer are:

- **RQ1:** What are the main drivers for cybersecurity governance in fintechs?
- **RQ2:** What are the challenges in implementing cybersecurity governance?

1.6. Rationale of the study

Research specific to cybersecurity practices in South African fintechs is currently limited yet these organisations play an increasingly strategic role in the country's socio-economic development plans. By identifying the drivers for cybersecurity and the challenges in implementing cybersecurity governance programmes within fintechs, this study will provide insights that fintechs can use to enhance their cybersecurity strategies, guide regulators in their interaction with fintechs, and lastly, contribute to the cybersecurity body of knowledge.

1.7. Delimitation of the study

This research will focus on fintech companies in South Africa. As the name implies, fintechs operate are at the intersection of financial services and modern information technology. Compared to traditional financial service providers, fintechs are founded on agile and innovative operating models that leverage data and cutting-edge technology such as cloud computing, big data analytics, application programming interfaces (APIs), mobile-first platforms and more recently, artificial intelligence (AI). However, while traditional providers have developed robust cybersecurity protocols over time, fintechs, particularly emerging ones, have historically faced challenges due to business constraints and a focus on rapid scaling, leading to less mature cybersecurity structures. Further, the research does not extend beyond the borders of South Africa. The decision to limit the study to South African fintechs is based on the country's relatively mature technology, financial, and regulatory systems compared to other African nations. Expanding the geographic scope would introduce considerable variability which would dilute the depth of analysis.

1.8. Definition of keywords

Cybersecurity	The process of protecting information by preventing, detecting, and responding to attacks (NIST, 2018).
Fintechs	Companies that rely primarily on technology and cloud services—and less so on physical locations—to provide financial services to customers (McKinsey, 2024). These companies typically do not possess the core licenses legislated within their industry (Williamson, 2024).
Governance	A framework of rules, practices, and processes to direct, control, and bring accountability in an organisation (Bevir, 2008).

Table 1.1 Definition of keywords.

1.9. Structure of the article

Chapter 1 introduces the research topic, outlines the research objectives and questions, and defines key terms. **Chapter 2** provides a review of the relevant literature on fintech, cybersecurity risks, and cybersecurity governance. **Chapter 3** outlines the research methodology, detailing the research approach, data collection methods, and data analysis strategies. **Chapter 4** presents and analyses the results of the study. **Chapter 5** concludes the research by summarising the key findings, offering recommendations, and outlining limitations and areas for future research.

2. Chapter 2: Literature review

2.1. Introduction

This chapter reviews the literature on fintech, fintech companies, and the key drivers and challenges related to cybersecurity. Additionally, it introduces the analytical framework that underpins the research.

2.2. Empirical literature review

2.2.1. Fintech overview

The term “fintech” is commonly associated with startup businesses that disrupt the status quo in financial services through technology-backed offerings (Murinde et al., 2022). However, the concept is more accurately described as a process that involves the application of information technologies in the financial services sector (Arner et al., 2015). Fintech therefore extends beyond these disruptive startups. Fintech has evolved over three generations marked by the shift from analogue to digital transmission for exchanging financial information from 1866 triggered by the laying of the Transatlantic cable systems, the development of digital financial services (DFS) in the late 1980s, and the democratisation of DFS post the global financial crisis of 2008 (GFC) (Arner et al., 2015). The organisations referred to as “fintechs” or the “fintech industry” in contemporary literature and practice are therefore businesses established in the current “fintech 3.0” era. Williamson (2024) provides a further distinction between fintechs and “traditional” service providers describing fintechs as entities operating without the core licences that are typically required within their industry. For example, in the South African context, new participants in the banking industry such as Bank Zero, Discovery, TymeBank are not considered fintechs despite their establishment in the “fintech 3.0” era and digital products because they possess the core licenses in the banking sector.

Fintech products leverage innovative business models, deriving a competitive advantage from the integration of innovative technologies such as artificial intelligence (AI), blockchain, cloud services, and big data (Buckley et al., 2019). These technologies enable products like digital banking platforms, which use AI and big data to offer personalised financial advice in the deposits and lending markets, and digital wallets and e-money systems, which streamline transactions using blockchain technology in the payments and settlements markets (Ehrentraud & Ocampo, 2020). Unencumbered by legacy systems and often facing less stringent regulatory

pressures, fintechs can introduce new products more rapidly than incumbents (Arner et al., 2015; Barberis et al., 2017; Lee & Shin, 2018).

The drivers for fintech adoption vary between regions and countries. In western countries, fintechs emerged due to a new regulatory environment after the GFC (Arner et al., 2015). In contrast, the development of fintechs in Africa has been due to the economic opportunities enabled by increased internet access and mobile phone penetration (Arner et al., 2015; Lee & Shin, 2018). Fintechs have brought value to the consumer through speed and convenience. In South Africa, specific factors driving penetration include usefulness, economic benefit, trust, and social influence (Slazus & Bick, 2022). However, as fintechs grow, they encounter various challenges and risks, including cybersecurity risk.

2.2.2. Cybersecurity risk and cybersecurity governance drivers and challenges

Cybersecurity risk is a function of digitalisation. As organisations increase the integration of information technology within their operations, the risk of cybersecurity incidents increases. By definition, cybersecurity risks are "operational risks to information and technology assets that have consequences affecting the confidentiality, availability, or integrity of information or information systems." (Cebula & Young, 2010, p. 1). These risks stem from four sources: the actions of people, failure in systems and technology, failure of internal processes, and events in the organisations' external environment (Cebula & Young, 2010). The consequences of these risks include data and privacy breaches, disruption of services, and identity theft (Aldasoro et al., 2020). Expressed financially, the impact of cybersecurity risks reduces profitability through the dual impact of decreased revenue and increased costs. Limiting the financial impact thus appears as the primary driver for cybersecurity efforts.

Expanding on the concept of impact as a financial quantity, Freund and Jones (2015) consider this impact as "loss" and categorise these losses into primary and secondary types. Primary losses encompass direct financial outlays related to productivity decline, incident response activities, and asset replacement. Secondary losses, on the other hand, capture the broader strategic consequences, including a decline in competitive advantage, potential regulatory fines and judgments, and reputational damage.

Biener et al. (2014) found that the losses from each cybersecurity risk source are relatively similar; however, the frequency of incidents varies significantly, with human actions

disproportionately accounting for 90% of incidents. Further, within this category, cybercrime poses the most serious threat as it occurs more frequently than inadvertent incidents (Biener et al., 2014; Brush & Cobb, 2021). Infringements conducted by cybercriminals include unauthorised access, deploying viruses and malware, launching denial-of-service attacks, computer fraud, and using phishing schemes carried out by hackers, hacktivists, and nation-states for the purposes of financial gain, social / political protest, and espionage (Ayofe & Oluwaseyifunmitan, 2009; Șcheau et al., 2022).

In South Africa, the extent of losses due to cybersecurity incidents in fintechs and in general is unknown (Africa Check, 2018). Pieterse (2021) notes that South African organisations do not have an incentive to report cybercrime due to the risk of "double jeopardy" through secondary losses, particularly, reputational damage. Further, even when cybercrime activities are reported, law enforcement agencies do not presently disclose the related statistics (Pieterse, 2021). Consequently, "related industry" reports offer the closest proxy for estimating loss. For instance, the South African Banking Risk Information Centre (SABRIC, 2023) reported over R740 million in digital banking losses in 2022, equating to roughly R2 million per day. Even though these figures likely understate the true cost as they do not include inputs from other, non-direct forms of loss, Akinbowale et al. (2023) concluded that the impact of cybersecurity incidents on the South African banking industry is substantial. Given the high level of interdependence between fintechs and traditional institutions, the potential consequences of cybersecurity risks on fintechs could be even more catastrophic as they have greater exposure because of a higher reliance on information and technology within their operations (Buckley et al., 2019; Jamilov et al., 2021; KPMG, 2019).

The ramifications of cybersecurity risks extend into the broader fintech ecosystem. Other affected parties include customers of fintechs and the broader financial services industry (KPMG, 2019). In addition to financial losses, customers may experience emotional distress, fear, and even moral harm due to fintech-related cybercrime (Tsakalidis & Vergidis, 2019). This vulnerability aligns with customer perceptions of security by Lucidity Insights (2023), which revealed that 70% of surveyed Africans across 10 countries lacked confidence in the adequacy of security controls protecting their personal data within fintech products. While the inclusion of South Africa within this sample is unknown, these findings corroborate the research by Slazus and Bick (2022) in South Africa, which identified perceived risks (including cybersecurity) as a barrier to fintech adoption among consumers.

In the broader financial services sector, cybersecurity risks in fintechs are a source of systemic risks. This is due to the interdependencies that exist in the sector, where institutions rely on each other's infrastructure and services (Buckley et al., 2019; KPMG, 2019). For instance, integrations with registered banks enable fintech services in the payments industry (Payments Association of South Africa [PASA], 2023). Similarly, insurtech startups rely on underwriting provided by established players. Further, the industry exhibits a tendency towards "cyber monoculture" where many firms utilise the same technology solutions which creates a domino effect: a security breach in one organisation can rapidly progress to others (Buckley et al., 2019). While systemic risk events may be infrequent, their potential impact is severe. In response, regulators are taking a keen interest in the development of the fintech space. Their primary concerns are maintaining financial stability and integrity, protecting consumers, and fostering financial inclusion (Buckley et al., 2019).

In response to cybersecurity risks, organisations engage in several interrelated practices collectively termed cybersecurity governance. More formally, cybersecurity governance refers to "the set of policies, procedures, and standards that an organisation puts in place to ensure the protection of its information systems and data." (Mijwil et al., 2023, p. 3). It forms part of the enterprise governance, risk, and compliance (GRC) strategy, which coordinates people, processes, and technology in the deployment of various controls with the overall goal of managing cybersecurity risks at levels acceptable to the organisation (Akridge, 2020; Teoh et al., 2018). The high-level activities of cybersecurity governance include prevention, detection, and responding to threats (Akridge, 2020).

Within fintechs, achieving the objectives of these activities is increasingly difficult because of a combination of several factors. Firstly, fintech services are designed in such a way that the frequency of interaction between their data and technology assets, and threat actors is higher compared to incumbent providers, making them particularly vulnerable (Arner et al., 2015; Freund & Jones, 2015). This vulnerability is further exacerbated by several insecure practices, including storing sensitive data on client-side devices that do not have stringent controls. Secondly, threat actors are exploiting the decreased skill levels and resources required to carry out attacks as a result of AI, cloud and automation technologies, and the availability of tools and services designed to exploit others on darknet digital marketplaces (Haynes, 2025; Świątkowska, 2020). This is further fuelled by the anonymity offered by the internet, which decreases the chances of being caught (Świątkowska, 2020). Lastly, within fintechs themselves, there is a lack of cybersecurity risks awareness among employees (Kuraku et al.,

2023), a shortage of cybersecurity talent in the country (Kruger et al., 2022), and limited time, funding and other resources within the cybersecurity function (de Jager et al., 2023).

2.3. Analytical framework

2.3.1. Conceptual framework

Figure 2.1 illustrates the interconnected relationships between the fundamental elements of people, processes, and technology and their impact on the core cybersecurity functions. These cybersecurity functions, in turn, directly influence the overall cybersecurity risk posture of the fintech organisation. Notably, challenges and weaknesses within the people, processes, and technology components (such as inadequate awareness or integration issues) can significantly compromise the efficiency and effectiveness of the cybersecurity functions, amplifying the fintech's exposure to cybersecurity risk.

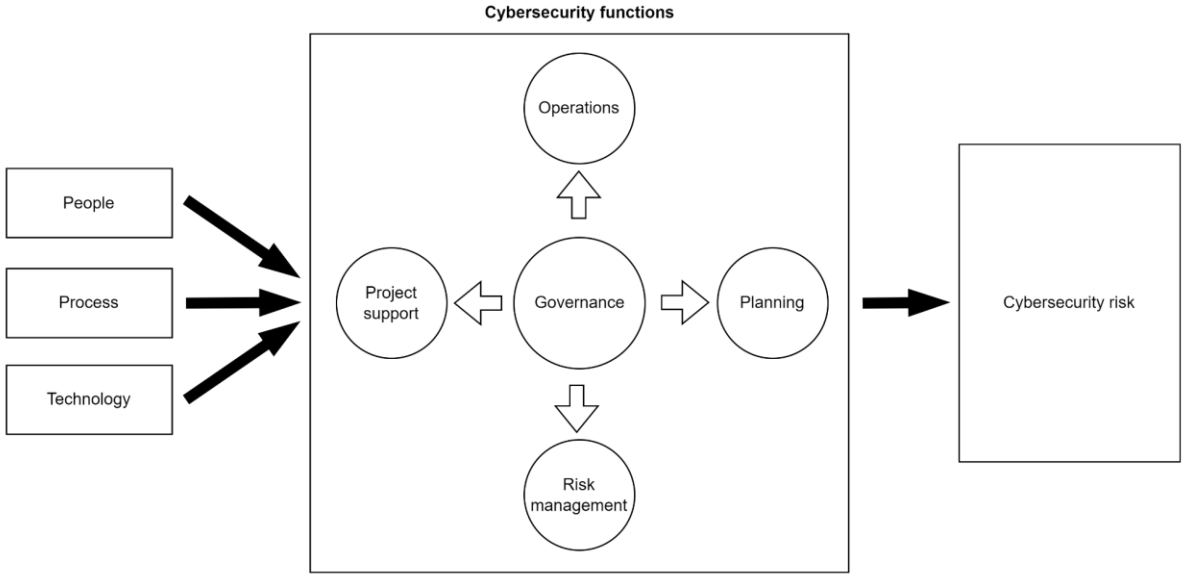

Figure 2.1 Conceptual framework.

2.4. Conclusion

While the literature highlights the significant impact of cybersecurity incidents on fintechs and the critical role of cybersecurity governance for their success (Ehrentraud & Ocampo, 2020; Oladipo et al., 2024), research specific to the South African fintech landscape remains limited. This study aims to address this gap by providing an in-depth analysis of the drivers and challenges of cybersecurity governance within this unique context.

3. Chapter 3: Research methodology

3.1. Introduction

This chapter provides details about the methodology, targeted population, and the sampling techniques employed to investigate the research objectives. Additionally, the chapter describes the research instrument and the methods that were used to analyse the collected data, and it concludes by outlining the limitations and quality assurance measures of the research. **Figure 3.1** illustrates the overall research framework**.**

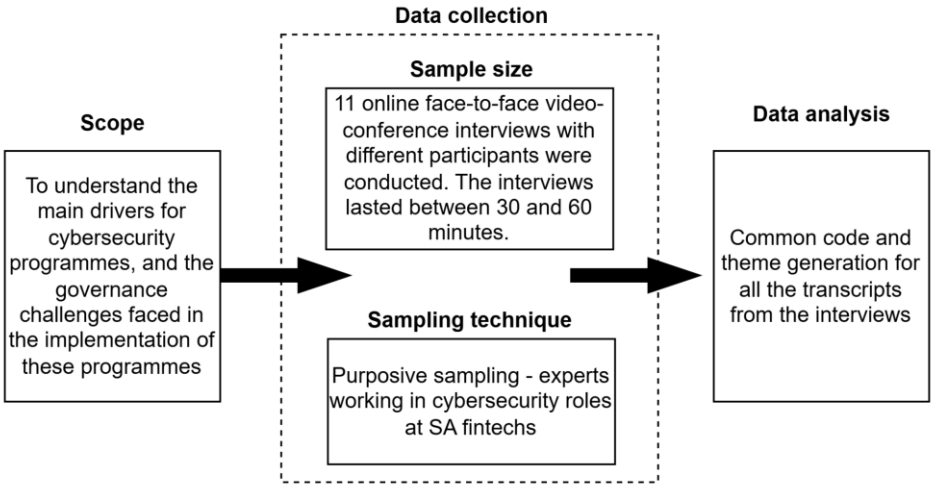

Figure 3.1 Research framework.

3.2. Research approach and design

The aim of this research was to gain a comprehensive understanding of the key drivers behind cybersecurity practices and the challenges associated with their implementation. To achieve this, a qualitative approach was adopted. Qualitative assessments are well suited for evaluating cybersecurity governance at a programmatic level as they can offer deeper insights compared to quantitative methods (Schroeder et al., 2021).

The research design is based on the case study approach. A comparative analysis of multiple fintechs enabled cross-case analysis and identification of patterns and themes.

3.3. Research paradigm

A paradigm refers “to the foundational set of assumptions that shape the framework, theoretical approaches, and methodologies within which a group operates” (Saunders et al., 2023, p. 145).

Given that the research was qualitative in nature, using a small sample size and in-depth structured interviews within a complex subject area, it aligns with an interpretivist approach.

3.4. Data collection methods

3.4.1. Population

The research population, defined as the complete set of cases or elements under consideration (Saunders et al., 2023), comprises fintech organisations in South Africa. Due to the lack of a centralised registry, a universally accepted definition of "fintech", and other contributing factors (Schueffel, 2016), the precise number of fintechs in South Africa was unknown at the time of the research. Estimates from grey literature ranged from 121 to 203 (**Table 3.1**). The research adopted the conservative estimate of 121 as the population size.

Source	Genesis Analytics (2019)	Findexable (2021)	Disrupt Africa (2023)
Fintechs identified	203	121	140

Table 3.1 Number of fintechs identified by different sources in grey literature.

3.4.2. Sample and sampling method

The sample refers to the subset of the population chosen for data collection through a specific sampling method (Saunders et al., 2023). Purposive sampling, a non-random technique where participants are selected based on their knowledge and experience (Etikan et al., 2016), was employed to select participants for this research. Specifically, cybersecurity leaders in South African fintech companies were chosen, enabling the cost-efficient acquisition of high-quality data (Gill, 2020). Eleven interviews were conducted. Although the initial target was twelve, with three additional interviews planned as a stopping criterion, data saturation, as defined by Francis et al. (2010), was reached prior to the twelfth interview. Therefore, the sample size of eleven was deemed appropriate.

3.5. Research instrument

The research instrument was a peer-reviewed semi-structured interview designed to address the research questions. The use of a semi-structured interview facilitated the exploration of participants' thoughts, feelings, and beliefs regarding the research topic (Saunders et al., 2023).

The interview was organised in three sections. The first section focused on understanding the organisational context and key drivers of the cybersecurity function. The second section

explored organisation and challenges experienced across the five cybersecurity functions identified by Akridge (2020) i.e., governance, operations, planning, risk management, and project support—as they relate to people, process, and technology. Finally, participants were invited to share additional insights regarding cybersecurity within the South African fintech context. **Appendix A** contains the research instrument.

3.6. Data collection procedure

The data collection was conducted via synchronous, online, face-to-face video conferences using Microsoft Teams. This method was chosen for the convenience of both the interviewer and participants. Participants were informed of the recording and transcription process and provided their consent. Microsoft Teams' recording and automatic transcription features were utilised. Two participants chose not to activate their video cameras due to technical and personal reasons. The interviews lasted between 30 and 60 minutes.

3.7. Data analysis strategies and interpretation

Thematic analysis was employed to interpret the interview data. This approach is particularly well-suited to semi-structured interviews because it facilitates the identification of recurring themes and exploration of both similarities and differences in perspectives across the participants (Karatsareas, 2022). The six-step process of thematic analysis (familiarising with the data, generating initial codes, searching for themes, reviewing themes, defining and naming themes and producing the report) outlined by Braun and Clarke (2006) was followed.

To gain familiarity with the data, the automatically generated transcripts were reviewed and corrected for inaccuracies. This process included listening to the recordings and comparing them to the transcripts. A combination of manual coding and analysis, aided by the NotebookLM AI tool, was employed to generate codes and identify themes. The themes were then categorised according to the research objectives.

3.8. Limitations

This study acknowledges the potential for self-serving bias on the part of interviewees. The semi-structured interview format may inadvertently position the interaction as an evaluation of the interviewee's performance. This could incentivise participants to downplay challenges within their area of control.

3.9. Quality assurance

3.9.1. External validity

External validity refers to the extent to which research findings can be generalised to other contexts (Saunders et al., 2023). This research focused specifically on South African fintech, where the implications of cybersecurity risks may differ from those in other sectors, including the broader financial services industry. Therefore, the findings may not be directly applicable to industries with characteristics distinct from those of fintech. Additionally, because the research participants were primarily drawn from the payments sector, the generalisability of findings in other fintech sectors is potentially limited.

3.9.2. Internal validity

Internal validity refers to the research instrument's ability to measure what the researcher intended to measure (Saunders et al., 2023). The internal validity of the findings was strengthened by several factors. The sample size, while relatively small, was deemed sufficient as data saturation was reached, therefore, additional interviews were unlikely to yield new themes or insights. Furthermore, the researcher employed reflective practices throughout the analysis process to mitigate personal biases and ensure a more objective interpretation of the data.

3.9.3. Reliability

Reliability refers to the consistency of data collection (Saunders et al., 2023). In this domain-specific study, reliability hinged on the participants' knowledge of cybersecurity within the fintech context. The findings demonstrated internal consistency, as participants largely responded to the questions in a similar manner. However, given the evolving nature of both cybersecurity and fintech, and the varying priorities businesses attach to issues around cybersecurity, the research instrument may yield different results if applied at a different time or in a different context.

3.10. Ethical assurance

The researcher obtained ethical clearance from the University of the Witwatersrand Ethics Committee (protocol number WBS/BA2696297/409) before commencing data collection. A key condition of this approval was the guarantee of participant confidentiality, which was strictly upheld throughout the research process. Beyond the university’s requirements, established ethical frameworks specific to cybersecurity were used to guide the research.

Specifically, the principalist approach (Formosa et al., 2021) was followed with an emphasis on principles derived from common-sense ethics and professional practices (Loi & Christen, 2020). The research adhered to the principles of respect for persons, justice, and beneficence as outlined in the Menlo Report (Dittrich & Kenneally, 2012).

Prior to the interviews, participants were informed of the research objectives and provided their consent to participate. To ensure privacy and security, all collected data were anonymised. The data has been securely archived on a dedicated, password-protected workstation. All data will be permanently deleted two years after the study is completed.

4. Chapter 4: Presentation and analysis of results

4.1. Introduction

This chapter presents a qualitative analysis and discussion on the data collected during the study. Thematic analysis was used to analyse the transcripts generated from the structured interviews. The chapter begins with an overview of the sample characteristics, followed by a presentation of the findings, which are organised in alignment with the research objectives in **Chapter 1**.

4.2. Description of the sample

Eleven participants were individually interviewed to collect the data that addressed the research questions. Each participant was a male and full-time employee at a fintech company operating in South Africa and identified themselves as the individual primarily responsible for the organisation's cybersecurity function. **Table 4.1** provides an overview of the interviewees, including their identifiers, roles, and years of experience in cybersecurity.

Identifier	**Role at fintech**	**Cybersecurity experience**
Participant 1	Information Security Manager	12 years
Participant 2	Chief Information Security Officer	20 years
Participant 3	DevOps Manager	17 years
Participant 4	Software Developer	Undisclosed
Participant 5	Chief Technology Officer	20 years
Participant 6	Security Specialist	8 years
Participant 7	Information Security Manager	19 years
Participant 8	Chief Technology Officer	Undisclosed
Participant 9	Operations Manager	6 years
Participant 10	Head of Information Security	20 years
Participant 11	Information Technology Director	20 years

Table 4.1 Description of the study's participants

4.2.1. Fintech type

Most participants were employed by fintech companies primarily engaged in payment-related services, including transaction processing, payment gateways, and payment solutions. Out of eleven, three participants (**4, 8, and 11**) worked in other areas of fintech. The over-representation of payment-related services in the sample is consistent with the overall composition of the fintech industry. This distribution is illustrated in **Figure 4.1**.

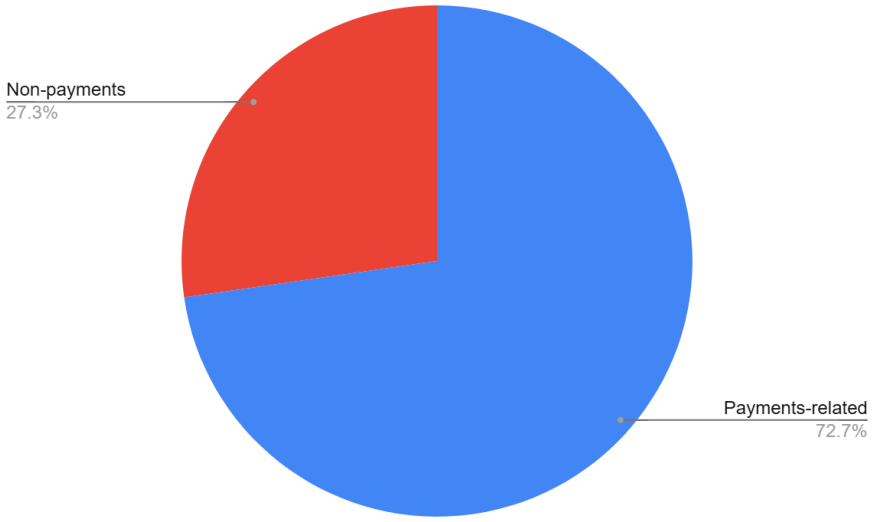

Figure 4.1 Participant's organisation fintech type (payments vs non-payments)

4.2.2. Fintech size

The size of the fintech companies represented by the participants varied considerably. Some participants were sole employees of their respective companies, while others worked for organisations with more than 250 employees. **Figure 4.2** illustrates the distribution of these companies based on employee count.

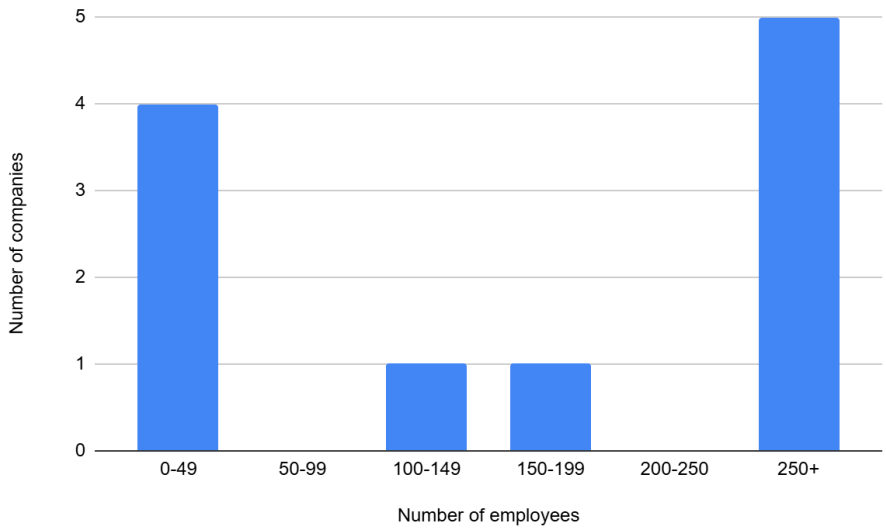

Figure 4.2 Number of companies by employees.

4.2.3. Organisation of the cybersecurity function

All participants confirmed that their organisations had formal cybersecurity policies in place. They also reported using a range of frameworks to guide their cybersecurity governance, including PCI DSS (primarily in payment systems), the NIST Cybersecurity Framework, ISO/IEC 27001, and the CIS Critical Security Controls. The degree to which each framework was implemented, however, varied across participants.

4.2.4. Participant's role and cybersecurity experience

The participants held roles ranging from security specialists and managers to C-level executives, had cybersecurity experience ranging from 6 to over 20 years, with two participants' experience levels undisclosed. Four (36%) of the eleven participants were solely dedicated to cybersecurity, while the remaining seven (64%) held additional roles alongside their cybersecurity responsibilities. This distribution is illustrated in **Figure 4.3**.

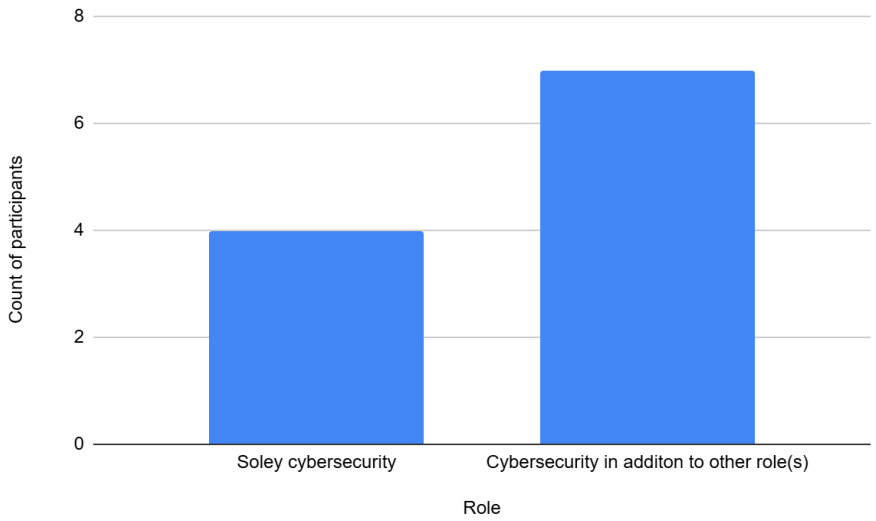

Figure 4.3 Participant's roles within fintech.

4.3. Presentation of the results

This section presents an analysis of the data collected from the participants grouped in themes under the related research questions, i.e., what are the main drivers for cybersecurity governance in fintechs, and what are the challenges in implementing cybersecurity governance?

4.3.1. Drivers for cybersecurity governance

4.3.1.1. Theme 1: The primacy of compliance and regulation

A significant driver for cybersecurity governance was the need to comply with external regulations and contractual agreements to mitigate non-negotiable compliance risks. All participants working in the payments fintech sector (73% of participants) indicated that Payment Card Industry Data Security Standard (PCI DSS) compliance was a mandatory requirement to operate in that industry. As a result, achieving compliance was the primary responsibility for cybersecurity personnel.

Participant 7 stated *"My main responsibility is to ensure that our company complies with PCI DSS [because] to be blunt, if you are not PCI DSS compliant, then you do not have clients."*

Participant 1 stated *"What is expected of me is to ensure that PCI compliance is maintained… I think if my organisation had it any other way, they would not hire a dedicated security person - the only reason why they do it is because it is a requirement in PCI DSS."*

Participant 6 similarly stated *"We have certain requirements that we need to adhere to from the Payment Card Industry… We concentrate solely on the PCI requirements."*

In addition to PCI DSS, the Protection of Personal Information Act (POPIA) was referenced either directly or indirectly in all but one interview (**Participant 7**). Another regulation that was referenced (albeit only once) was the South African Reserve Bank's (SARB) directive in respect of cybersecurity and cyber-resilience within the national payment system.

Participant 2 stated that *"One of the things that we are now governed by is the South African Reserve Bank directive which speaks to cybersecurity and cyber resilience."*

Fintechs that operate beyond South African borders are also regulated by the local legislation around cybersecurity in those geographies.

Participant 5, whose organisation operates across the continent, stated that local regulations in the various countries needed to be adhered to. These regulations, however, are similar to the PCI requirements, indicating that the effort needed to comply is not very significant.

4.3.1.2. Theme 2: Cybersecurity as part of enterprise risk management

In addition to addressing compliance risk, cybersecurity governance is also part of a more holistic approach to risk management. This is particularly true in larger fintechs and those that are not in the payments ecosystem and thus are not subject to PCI DSS. Cybersecurity governance was seen as critical to ensure business continuity and for safeguarding reputational risk.

Participant 11 viewed cybersecurity as no different from other organisational risks, and thus it fell under the enterprise risk function. He stated that *"Cybersecurity is just another risk, it is not necessarily any more relevant than health and safety risk, finance risk, foreign exchange risk. So cybersecurity governance, in my opinion, only works if you have committees and specialities working under a normal enterprise risk management framework."*

Participant 2 stated that the operations of a fintech company took place in the digital space, therefore *"Cyber risk is pretty much the number one risk on our enterprise risk register."*

Similarly, and perhaps more simply, **Participant 5** asserted that cybersecurity governance was necessary because "*If you get hit, you will vanish.*"

Some participants indicated that the reputational damage as a result of cybersecurity risk was potentially irreparable.

Participant 5 and **Participant 7** aptly summarised this point by emphasising the critical importance of reputation, stating, *"It's all about your reputation"* and *"Reputation is everything"* respectively.

4.3.1.3. Theme 3: Cybersecurity as a differentiator

A final but less prevalent driver for cybersecurity governance was that it provides a competitive advantage.

Participant 8 stated that robust cybersecurity controls were necessary to prevent breaches not because of the legal repercussions but because of the need to protect competitiveness — *"it is paramount that we do not get data breaches, that we do not have data leaks … it would create serious competitive issues."*

4.3.2. Challenges in cybersecurity governance

4.3.2.1. Theme 1: Shortage of cybersecurity capacity and talent

Although not expressed by all participants, the shortage of cybersecurity capacity and talent was a recurring theme. Several participants stated that there was a lack of expertise in areas such as risk management, incident response, and secure development practices.

Reflecting on the workload of his team, **Participant 6** noted that *"Lots of guys are overwhelmed."* highlighting capacity concerns. Similarly, while acknowledging the business constraints, **Participants 2, 7, and 10** expressed that their current teams were inadequately staffed to cope with the workload.

For **Participant 8,** cybersecurity operations constituted a shared responsibility, as his organisation did not have personnel solely focused on it. He also noted that it would be a challenge to find a full-time cybersecurity officer who *"really covers all the bases"*. Similarly, **Participants 1, 3, 4, 5, and 9** reported that they performed other roles in addition to cybersecurity.

Participant 5 emphasised the challenge of retaining cybersecurity talent amidst high industry demand, noting that *"people tend to gain knowledge and experience and then leave after a couple of years."*

Participant 9 bemoaned the skills flight out of the country: *"I don't honestly think we have the skill in South Africa because most of the guys that I've met that have built the skills have left the country. A lot of them that I've dealt with have left for Ireland. And you know, we need those guys in the country — in the Fintechs themselves."*

As a mechanism to limit the impact of talent and capacity shortages, a common strategy that fintechs use is outsourcing aspects of the cybersecurity programmes to third parties. On the extreme end, **Participant 4's** organisation primarily relied on the cloud service provider's rails for the bulk of its cybersecurity controls. **Participants 1, 3, and 6** employed their Qualified Security Assessor (QSA) — the organisation that does PCI auditing in operational capacities. **Participants 5, 8, and 10** used third parties to perform specific or less frequent tasks.

4.3.2.2. Theme 2: Financial constraints

A lack of sufficient funding was identified as a significant challenge in implementing all the necessary cybersecurity solutions and applications to protect the businesses.

Participant 7 stated that budget constraints were the biggest challenge to being more security-focused: *"Funding is quite a big issue because as you know, information security does not necessarily generate income for every business that it tries to protect."*

Participant 9 also highlighted budgetary constraints as the main challenge in addressing cybersecurity, *"Because we are a small company, funding is a hold back."*

Similarly, when prompted what the biggest challenge was in being more effective, **Participant 6** stated *"Budget. I think that's honestly the main thing because as I say, once again it comes back to the cost to implement cybersecurity solutions. It is very expensive to implement solutions."*

Participant 5 stated *"Sometimes you need to allocate a budget for cybersecurity controls and operations and other stuff, and in case if you have a limited budget, sometimes you need to delay things or make things manual or depend on workloads. Until you have enough money to invest."*

4.3.2.3. Theme 3: Low value perceptions and lack of alignment

Some participants indicated that a level of tension existed in relationships and interactions between the cybersecurity function and the broader business. In this regard, two sub-themes

emerged: the value perception of cybersecurity and cybersecurity seen as a delaying agent in the time to market.

Commenting on the challenges faced when planning cybersecurity initiatives with the rest of the business, **Participant 7** said *"To be honest, the main issue is a soft one — to get the availability of some of the business owners because they have got their own priorities and KPIs that they need to meet."*

Participant 6 stated that there was a disconnect between the security team and other areas of the business, from his perspective: *"The other guys in IT, networking, and engineering understand security because they are aware [of the risks]. But the further you move away from that level, the higher you go in the company, when it comes to security, what they are seeing is money being thrown at something that there's no tangible evidence of. There's no recouping of that money. That's the perception."*

According to **Participant 2** *"one of the most difficult things to do is to effectively communicate what the actual risk is … unless we're able to effectively quantify risk in a monetary term, it's very difficult for those that aren't familiar with technology and with security principles as to what the actual impact is."*

Cybersecurity processes were also seen as working, increasing the time to market, which is particularly undesirable in fast-paced industries.

Participant 1 stated that his organisation prioritises speed over security: *"Since the company is going the Silicon Valley route and trying to be agile like most other companies, they value speed ahead of a lot of things. So when you do raise questions for them. They are just worried about delivery as opposed to security."*

Participants 2, 3, and 5 also highlighted the speed vs. security debate. As a result, one of the outcomes was that business and project participants may not be forthright with information required by cybersecurity to make informed assessments.

Participant 2 noted that *"Lack of transparency, lack of knowledge sharing, lack of documentation, lack of architecture. It makes it very difficult for us to really assess the security holes or gaps and to do accurate reviews if we don't have all the information."*

4.3.2.4. Theme 5: Evolving threat landscape

Participants noted that managing cybersecurity programmes has become increasingly challenging due to several threats within cyberspace. Key concerns include third party and supply chain risks, phishing attacks, and ransomware.

Participant 4 highlighted the challenges posed by the rapid pace of technological advancements, stating, *"The fast-evolving nature of security risks and cyber threats requires us to stay up to date with the latest threats."*

Similarly, **Participant 9** remarked that *"The pace of change is so fast, I don't know how anyone keeps up with that."*

Attacks also extend beyond the organisation, as highlighted by **Participant 1**: *"We've experienced attempted phishing where someone obtained the CEO's details from a data dump. While we're unsure of the dump's age, they used this information to try to contact our customers. Fortunately, we identified the threat quickly, as most of our customers are trained to validate and verify any changes before taking action."*

Concerned with the high number of third parties providing security services, **Participant 7** commented that *"The biggest challenge now is from an industry perspective. Number one is going to be a third-party risk assessment. I don't think a lot of the companies out there do proper third-party party risk assessments to ensure that the service providers they bring into their environments are security knowledgeable and evaluate their security posture".*

Regarding AI, **Participant 2** highlighted its growing prevalence and its ability to accelerate the operations of adversaries, noting that *"the threat actors are always going to be one step ahead."* **Participant 8** further emphasised how AI is enhancing the sophistication of phishing attacks, explaining, *"It is also becoming more difficult because, again, with AI, you can now have a video call with someone who doesn't exist, who looks like one of your colleagues and is asking you to do something on the computer. It is getting more and more difficult to keep things secure."*

4.4. Discussion

4.4.1. Drivers for cybersecurity governance

Research Question 1 sought to understand the drivers for cybersecurity governance in fintechs. Unsurprisingly, the research found that the drivers for cybersecurity governance in

fintechs were similar to those in other organisations, i.e., cybersecurity governance is rooted in risk management (Akridge, 2020; Slazus & Bick, 2022; Teoh et al., 2018). However, where Cebula and Young (2010) defined cybersecurity as a type of operational risk, the research found that the origins of cybersecurity risk can emanate from other areas of business, including compliance and finance. Consequently, fintechs tended to view cybersecurity risk according to their primary focus. For instance, fintechs providing payment-related services were primarily concerned with meeting the PCI DSS compliance objectives, while those providing credit services were mainly focused on limiting credit risk.

It is important to note that cybersecurity governance was not limited to addressing specific risks alone; rather, it extended across a broader spectrum of risks associated with the use of technology such as operational risks. This highlights the existence of a continuum between specific, targeted risks, and overarching technology-related risks within which fintechs operate. In this regard, the extent to which a fintech's cybersecurity approach is holistic—rather than focused on specific risks—seems to be strongly influenced by its size: larger fintechs typically adopt more comprehensive cybersecurity strategies, while smaller firms often concentrate on specific areas. This is congruent with Dinkova et al.'s (2023) research, which found that smaller firms often exhibit lower levels of cybersecurity maturity compared to their larger counterparts and are thus more susceptible to cybersecurity incidents. Although Dinkova et al. (2023) found no correlation between cybersecurity maturity and financial performance across a broader range of organisations, Goh et al. (2020), focusing specifically on financial institutions, including fintechs, found that cybersecurity incidents negatively impact financial performance. Consequently, smaller fintechs appear to carry a higher degree of cybersecurity risk.

4.4.2. Challenges in cybersecurity governance

Research Question 2 aimed to uncover the challenges confronting effective governance. The findings presented in the results highlight a series of interconnected challenges, with the most significant of these revolving around the threats emerging from a constantly changing external environment and the internal configuration (people, processes, and procedures) of fintech to defend against those threats.

The research found that the primary challenge in cybersecurity governance in South African fintechs was the lack of adequate financial resources to support cybersecurity initiatives. This mirrors findings from de Jager et al. (2023), whose research sample included participants from the broader South African IT landscape and highlighted financial constraints as a critical barrier

to effective cybersecurity implementation. The cybersecurity activities in fintechs, particularly those in the payments industry, were primarily focused on achieving PCI DSS compliance and meeting statutory requirements; as a result, some of these fintechs were not effectively managing cybersecurity beyond the compliance requirements.

In addition to financial resources, the research also found that there was a insufficient human capital resources allocated to cybersecurity operations. Contributing factors included budget constraints, and difficulties in hiring and retaining personnel in part due to skills flight out of the country. The latter echoes Kruger et al. (2022), who found that there was a shortage of cybersecurity talent in the country. As a result, some participants were performing cybersecurity functions in addition to other roles to cover gaps but leading to increased workloads and stress.

The disparity between the resources required and those allocated also implies that there is a degree of unmitigated risks, a portion of which appears to be unknowingly accepted due to the lack of understanding of these risks at the business level. Participants reported difficulties in articulating the potential impact from certain threats — a factor that likely hinders their ability to secure the resources required to implement the appropriate countermeasures. This seemed to stem from a lack of shared language regarding risk between cybersecurity and business. Another contributing factor to this issue was the hierarchical distance between cybersecurity managers and executives, where some cybersecurity leaders were three levels removed from the executive leadership, which may hinder effective communication and risk awareness.

Outsourcing cybersecurity functions has become a key strategy among many fintechs, partly as a response to the cybersecurity talent shortage described above. However, as Goh et al. (2020) point out, dependence on third parties introduces supply chain risks. Third party involvement can create new vulnerabilities, potentially compromising fintech operations. One participant highlighted this concern, noting that third party risk is among the largest unchecked threats facing fintechs. This perspective is echoed by Benaroch (2021), who found that incidents involving third parties often lead to greater financial losses. A recent example is the 2024 Crowdstrike outage, in which a reputable third-party security provider experienced a failure, causing widespread disruptions across multiple industries and resulting in estimated losses between $4 billion and $6 billion (George, 2024). By relying on unchecked third parties, fintechs are inadvertently increasing their exposure to risk.

The research also found that several technologies recognised as providing fintechs with competitive advantage such as AI, blockchain, cloud services, and big data, have not been widely applied within the cybersecurity function. While cloud computing and big data have seen some adoption, emerging technologies like AI and blockchain were underutilised. The reason for this might be the reactionary nature of businesses to cyber threats rather than a proactive approach (especially for those fintechs whose programmes are guided by compliance requirements), and linkages to the resourcing challenges indicated earlier. This gap, however, is concerning, especially as Świątkowska (2020) highlighted that adversaries are increasingly leveraging these very technologies to their advantage, for which, according to Haynes (2025), existing toolsets are limited against. As one participant pointed out, this dynamic places adversaries on the front foot, underscoring a need for cybersecurity functions to harness these tools to enhance defences.

4.5. Conclusion

This chapter explored the drivers for cybersecurity governance practices of South African fintechs and identified several key challenges experienced in the execution of cybersecurity programmes. Financial and human resource constraints, coupled with a lack of understanding of cybersecurity risks at the business level, hinder effective cybersecurity governance. Fintechs need to address these challenges to enhance their cybersecurity posture.

5. Chapter 5: Conclusion and recommendations

5.1. Introduction

The aim of the research was to evaluate the drivers and challenges of cybersecurity governance within the South African fintech sector. This was achieved through a qualitative approach, utilising semi-structured interviews with cybersecurity leaders in the fintech industry. In conclusion, this chapter summarises the key findings and provides practical recommendations for fintechs based on the study's insights. Additionally, it outlines potential avenues for future research.

5.2. Conclusion

The research found that South African fintechs face significant cybersecurity governance challenges, primarily due to financial and human resource constraints, as well as a lack of business-level understanding of cybersecurity risks. These challenges are further compounded by a rapidly evolving threat landscape and the complexities of managing third-party dependencies. While regulatory compliance serves as a foundational driver for cybersecurity measures, it is often seen as the sole objective rather than a starting point for more comprehensive security strategies.

5.3. Recommendations

Across all organisations, the levels of cybersecurity risks are proportional to the degrees of digitisation and digitalisation. Because fintechs operate entirely within the digital sphere, they are particularly susceptible to these risks. Therefore, effective risk management is essential to mitigate potential harm. Based on the research findings, fintechs are advised to implement the following recommendations:

The first recommendation is to establish executive oversight on the cybersecurity function to ensure proper attention and accountability. Cybersecurity should be considered as an organisational risk and as such, it requires the senior-level management for effectiveness. Several participants reported stalled or slow progress in implementing ISO/IEC 27001 certification and other governance-related projects. Executive oversight on such initiatives will provide the necessary sponsorship needed to facilitate their completion, thereby increasing the likelihood of success. Also, a reporting structure that directly connects cybersecurity to senior leadership is essential for proactive decision-making and a swift response to emerging risks.

A second recommendation is for cybersecurity leaders to adopt quantitative risk analysis frameworks. Examples of these include Factor Analysis of Information Risk (FAIR). Quantitative risk analyses are objective and will facilitate better communication of risks and establish a common understanding of cybersecurity issues between business actors and cybersecurity, and IT practitioners (Ramona, 2011; Watson & Bergman, 2023). This will lead to informed decision making, particularly for large investments into cybersecurity capabilities.

Thirdly, to address resource constraints, fintechs should leverage technology more effectively and distribute cybersecurity responsibilities across the organisation. Emerging technologies such as AI offer a wide range of applications in cybersecurity that can significantly enhance operations (Ansari et al., 2022). Additionally, adopting "shift-left" practices, such as DevSecOps, can help distribute cybersecurity responsibilities by equipping non-cybersecurity teams with the knowledge and tools to integrate security tasks into their workflows (Butter, 2024). This approach ensures that security is embedded early in the development process rather than being treated as an afterthought. Furthermore, fintechs—especially the smaller ones—should consider utilising fractional services, e.g., virtual Chief Information Security Officers (vCISOs), to access specialised expertise on a flexible basis and on more affordable terms. By combining technological innovation with a collaborative approach to cybersecurity, fintechs can strengthen their defences while optimising limited resources.

A fourth recommendation is that fintechs relying on third parties must implement thorough due diligence processes, including comprehensive risk assessments. The research found that outsourcing plays a critical role in the organisation and execution of cybersecurity teams and processes; however, this approach is not risk-free, as these third parties can become potential vectors for breaches. Additionally, there are potential conflicts of interest that must be accounted for where third parties are engaged in both audit and operational capacities simultaneously.

A fifth recommendation, for fintechs operating in the payments sector, is that while regulatory compliance establishes a critical baseline and addresses essential hygiene factors, it should not remain as the sole focus of cybersecurity efforts. To ensure robust protection, fintechs must adopt a more comprehensive approach by implementing end-to-end measures that protect the entire business ecosystem. This shift from compliance-centric strategies to holistic, business-wide coverage will better mitigate risks and enhance resilience in an increasingly complex digital landscape.

Lastly, for government, regulators, policymakers, and fintech accelerators: it is essential to offer cybersecurity standards and guidance, particularly to early-stage fintechs and non-payments fintechs that lack specific industry guidance and compliance obligations. Furthermore, because security is not generally viewed as a competitive differentiator and considering the potential systemic impact of cybersecurity incidents, these stakeholders should actively encourage and facilitate information and strategy sharing among fintechs and within the broader financial services sector. Such a collaborative approach to cybersecurity will benefit the industry and ultimately society.

5.4. Limitations and further research

This study acknowledges certain limitations. First, most participants were drawn from the payments sector of the fintech industry. While payments represent the most widespread application of fintech, the findings may not be generalisable to other sectors. Additionally, the study relied on qualitative data, which, while offering rich insights, introduce a degree of subjectivity that could influence interpretation.

Notwithstanding these limitations, this study provides valuable insights into the drivers and challenges of cybersecurity governance within South African fintechs. The findings can be used by fintechs, particularly those in the payments sector, to enhance their cybersecurity governance practices. Moreover, the research contributes to the growing body of cybersecurity research in South Africa, which at the time of writing, was considered limited. Further research could expand upon these findings by including a broader range of fintech companies and employing a mixed-methods approach to data collection.

References

Adeyoju, A. (2019). Cybercrime and Cybersecurity: FinTech's Greatest Challenges. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3486277

Africa Check. (2018, August 2). *Does South Africa rank third in the world for online crime, losing R2.2bn a year?* Africa Check. https://africacheck.org/fact-checks/reports/does-south-africa-rank-third-world-online-crime-losing-r22bn-year

Akinbowale, O. E., Klingelhöfer, H. E., & Zerihun, M. F. (2023). The assessment of the impact of cyberfraud in the South African banking industry. *Journal of Financial Crime*, *22*(2), 287–301. https://doi.org/10.1108/jfc-10-2022-0260

Akinlaso, I. M., Adediran, I. O., Diallo, A. K., & Mahomed, Z. (2019). Blockdentity: A future beyond digital identity. In U. A. Oseni & S. Nazim Ali (Eds.), *Fintech in Islamic Finance: Theory and Practice* (pp. 281–302). Routledge. https://www.iefpedia.com/english/wp-content/uploads/2019/12/EBOOK9250.pdf

Akridge, S. (2020, July 8). *Essential Functions of a Cybersecurity Program*. ISACA. https://www.isaca.org/resources/isaca-journal/issues/2020/volume-4/essential-functions-of-a-cybersecurity-program

Al_Duhaidahawi, H. M. K., Zhang, J., Abdulreda, M. S., Sebai, M., & Harjan, S. (2020). Analysing the effects of FinTech variables on cybersecurity: Evidence form Iraqi Banks. *International Journal of Research in Business and Social Science (2147- 4478)*, *9*(6), 123–133. https://doi.org/10.20525/ijrbs.v9i6.914

Aldasoro, I., Gambacorta, L., Giudici, P., & Leach, T. (2020). The drivers of cyber risk. *Www.bis.org*. https://www.bis.org/publ/work865.htm

Ansari, M. F., Dash, B., Sharma, P., & Yathiraju, N. (2022, September 1). *The Impact and Limitations of Artificial Intelligence in Cybersecurity: A Literature Review*. Papers.ssrn.com. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4323317

Apruzzese, G., Laskov, P., de Oca, E. M., Mallouli, W., Rapa, L. B., Grammatopoulos, A. V., & Franco, F. D. (2022). The Role of Machine Learning in Cybersecurity. *Digital Threats: Research and Practice*, *4*(1). https://doi.org/10.1145/3545574

Arner, D. W., Barberis, J. N., & Buckley, R. P. (2015). The Evolution of Fintech: a New Post-Crisis Paradigm? *SSRN Electronic Journal*, *47*(4). https://hub.hku.hk/bitstream/10722/221450/1/Content.pdf?accept=1,2015

Arner, D., Buckley, R., Charamba, K., Sergeev, A., & Zetzsche, D. (2022). Governing FinTech 4.0: BigTech, Platform Finance, and Sustainable Development. *Core.ac.uk*. https://core.ac.uk/display/519794656

Ayofe, A. N., & Oluwaseyifunmitan, O. (2009). TOWARDS AMELIORATING CYBERCRIME AND CYBERSECURITY. *IJCSIS) International Journal of Computer Science and Information Security*, *3*(1). https://arxiv.org/ftp/arxiv/papers/0908/0908.0099.pdf

Barberis, J. N., Zetzsche, D. A., Buckley, R. P., & Arner, D. W. (2017). From FinTech to TechFin: The Regulatory Challenges of Data-Driven Finance. *Core.ac.uk*. https://core.ac.uk/display/84929817

Benaroch, M. (2021). Third-party induced cyber incidents—much ado about nothing? *Journal of Cybersecurity*, *7*(1). https://doi.org/10.1093/cybsec/tyab020

Bevir, M. (2008). *Key Concepts in Governance*. SAGE.

Biener, C., Eling, M., & Wirfs, J. H. (2014). Insurability of Cyber Risk: An Empirical Analysis. *The Geneva Papers on Risk and Insurance - Issues and Practice*, *40*(1), 131–158. https://doi.org/10.1057/gpp.2014.19

Braun, V., & Clarke, V. (2006). Using Thematic Analysis in Psychology. *Qualitative Research in Psychology*, *3*(2), 77–101.

Brush, K., & Cobb, M. (2021, September). *What is cybercrime?* TechTarget. https://www.techtarget.com/searchsecurity/definition/cybercrime

Bu, Y., Li, H., & Wu, X. (2021). Effective regulations of FinTech innovations: the case of China. *Economics of Innovation and New Technology*, *31*(8), 1–19. https://doi.org/10.1080/10438599.2020.1868069

Buckley, R. P., Arner, D. W., Zetzsche, D. A., & Selga, E. (2019, November 18). *The Dark Side of Digital Financial Transformation: The New Risks of FinTech and the Rise of TechRisk*. Papers.ssrn.com. https://ssrn.com/abstract=3478640

Butter, K. (2024). *Shifting security left: A qualitative study*.

Callen-Naviglia, J., & James, J. (2018). FINTECH, REGTECH AND THE IMPORTANCE OF CYBERSECURITY. *Issues in Information Systems*, *19*(3), 220–225. https://doi.org/10.48009/3_iis_2018_220-225

Cebula, J., Popeck, M., & Young, L. (2014). *A Taxonomy of Operational Cyber Security Risks Version 2*. https://insights.sei.cmu.edu/documents/2273/2014_004_001_91026.pdf

Cebula, J., & Young, L. (2010). *A Taxonomy of Operational Cyber Security Risks*. https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=f5610185253e64358fdf32b35855780f4cdf732f

Chaudhry, S. M., Ahmed, R., Huynh, T. L. D., & Benjasak, C. (2022). Tail risk and systemic risk of finance and technology (FinTech) firms. *Core.ac.uk*. https://core.ac.uk/display/478094015

Christou, G., & Raska, M. (2021). Cybersecurity. *The European Union in International Affairs*, 209–230. https://doi.org/10.1007/978-3-030-69966-6_10

Coetzee, J. (2018). Strategic implications of Fintech on South African retail banks. *South African Journal of Economic and Management Sciences*, *21*(1). https://doi.org/10.4102/sajems.v21i1.2455

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. *Technology Innovation Management Review*, *4*(10). https://www.timreview.ca/article/835

Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: A systematic review of data availability. *The Geneva Papers on Risk and Insurance - Issues and Practice*, *47*(3). https://doi.org/10.1057/s41288-022-00266-6

Cybersecurity Ventures. (2020). *Cybercrime To Cost The World $10.5 Trillion Annually By 2025*. https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/

de Jager, M., Futcher, L., & Thomson, K.-L. (2023). An Investigation into the Cybersecurity Skills Gap in South Africa. *IFIP Advances in Information and Communication Technology*, 237–248. https://doi.org/10.1007/978-3-031-38530-8_19

Didenko, A. (2017). *Regulatory challenges underlying FinTech in Kenya and South Africa*. https://www.biicl.org/documents/1814_regulation_of_fintech_in_kenya_and_south_africa_v_1.pdf

Didenko, A. (2018). Regulating FinTech: Lessons from Africa. *San Diego International Law Journal*, *19*(2), 311. https://digital.sandiego.edu/ilj/vol19/iss2/5/

Dinkova, M., El-Dardiry, R., & Overvest, B. (2023). Should firms invest more in cybersecurity? *Small Business Economics, 63*. https://doi.org/10.1007/s11187-023-00803-0

Disrupt Africa. (2023). *Finnovating for Africa: Reimagining the African financial services landscape*. https://disruptafrica.gumroad.com/l/tnnjib.

Dittrich, D. & Kenneally, E. (2012). The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research U.S. Department of Homeland Security,. Retrieved , from https://catalog.caida.org/paper/2012_menlo_report_actual_formatted

Ebrahim, R., Kumaraswamy, S., & Abdulla, Y. (2021). FinTech in Banks: Opportunities and Challenges. In *Innovative strategies for implementing FinTech in banking* (pp. 100–109). IGI Global.

Ehrentraud, J., & Ocampo, D. (2020). *Policy responses to fintech: a cross-country overview*. https://www.bis.org/fsi/publ/insights23.pdf

Etikan, I., Musa, S. A., & Alkassim, R. S. (2016). Comparison of Convenience Sampling and Purposive Sampling. *American Journal of Theoretical and Applied Statistics, 5*(1), 1–4. https://doi.org/10.11648/j.ajtas.20160501.11

Faya, M., & Ogbuefi, N. (2019, March 22). *Cybersecurity in the Age of FinTech and Digital Business*. Papers.ssrn.com. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3606866

Ferguson, K. K., Soutter, L., & Neubert, M. (2019). Digital payments in Africa - how demand, technology, and regulation disrupt digital payment systems. *International Journal of Teaching and Case Studies*, *10*(4), 319. https://doi.org/10.1504/ijtcs.2019.103771

Financial Stability Board. (2017). Financial Stability Implications from FinTech. In *fsb.org*. https://www.fsb.org/wp-content/uploads/R270617.pdf

Findexable. (2021). *Africa Fintech Radar*. Findexable. https://findexable.com/africa-fintech-radar/

Fintech Times. (2022). *The Fintech Times FINTECH: Middle East & Africa 2022*. https://issuu.com/fintechtimes/docs/the_fintech_times_fintech_middle_east_africa_202

Florackis, C., Louca, C., Michaely, R., & Weber, M. (2022). Cybersecurity Risk. *The Review of Financial Studies*, *36*(1). https://doi.org/10.1093/rfs/hhac024

Formosa, P., Wilson, M., & Richards, D. (2021). A principlist framework for cybersecurity ethics. *Computers & Security*, *109*. https://doi.org/10.1016/j.cose.2021.102382

Francis, J. J., Johnston, M., Robertson, C., Glidewell, L., Entwistle, V., Eccles, M. P., & Grimshaw, J. M. (2010). What Is an Adequate Sample size? Operationalising Data Saturation for theory-based Interview Studies. *Psychology & Health*, *25*(10), 1229–1245. https://doi.org/10.1080/08870440903194015

Freund, J., & Jones, J. (2015). *Measuring and managing information risk : a fair approach*. Elsevier, Cop.

Genesis Analytics. (2019). *Fintech Scoping in South Africa*. https://genesis.imgix.net/uploads/downloads/Fintech-scoping-in-South-Africa.pdf

George, S. (2024). When Trust Fails: Examining Systemic Risk in the Digital Economy from the 2024 CrowdStrike Outage. *Partners Universal Multidisciplinary Research Journal*, *1*(2), 134–152. https://doi.org/10.5281/zenodo.12828222

Gill, S. L. (2020). Qualitative Sampling Methods. *Journal of Human Lactation*, *36*(4), 579–581. https://doi.org/10.1177/0890334420949218

Goh, J., Kang, H., Xing Koh, Z., Way Lim, J., Wei Ng, C., Sher, G., & Yao, C. (2020). Cyber Risk Surveillance: A Case Study of Singapore. *IMF Working Papers*, *20*(28). https://doi.org/10.5089/9781513526317.001

Goyal, D., Varma, R., Rada, F., Pande, A., Jauregui, J., Corelli, P., Tripathi, S., Sénant, Y., Dab, S., Erande, Y., Choi, J., Koserski, J., Carrubba, J., Morris, N., Rotman, F., Risley,

M., & Suri, S. (2023). Global Fintech 2023: Reimagining the Future of Finance. In *BCG Global*. https://www.bcg.com/publications/2023/future-of-fintech-and-banking

Griffiths, J. (2016). Cyber Security as an Emerging Challenge to South African National Security. In *www.proquest.com*. https://www.proquest.com/dissertations-theses/cyber-security-as-emerging-challenge-south/docview/2901492962/se-2?accountid=15083

Haynes, A. (2025, January 27). *AI security posture management will be needed before agentic AI takes hold - Help Net Security*. Help Net Security. https://doi.org/10/16113940/ai-1500-face

Hua, X., & Huang, Y. (2020). Understanding China's fintech sector: development, impacts and risks. *Core.ac.uk*. https://core.ac.uk/display/334410228

Hussain, A., Mohamed, A., & Razali, S. (2020). A Review on Cybersecurity: Challenges & Emerging Threats. *Proceedings of the 3rd International Conference on Networking, Information Systems & Security*. https://doi.org/10.1145/3386723.3387847

International Criminal Police Organization. (2021). *African Cyberthreat Assessment Report 2021*. https://www.interpol.int/en/content/download/16759/file/AfricanCyberthreatAssessment_ENGLISH.pdf

International Organization for Standardization. (2021, March 25). *Information technology - Cybersecurity - Overview and concepts (ISO Standard No. 27100:2020)*. ISO. https://www.iso.org/standard/72434.html

Jagtiani, J., & John, K. (2018). Fintech: The Impact on Consumers and Regulatory Responses. *Journal of Economics and Business*, *100*, 1–6. https://doi.org/10.1016/j.jeconbus.2018.11.002

Jamilov, R., Rey, H., & Tahoun, A. (2021, June 1). *The Anatomy of Cyber Risk*. National Bureau of Economic Research. http://www.nber.org/papers/w28906

Javaheri, D., Fahmideh, M., Chizari, H., Lalbakhsh, P., & Hur, J. (2024). Cybersecurity threats in FinTech: A systematic review. *Expert Systems with Applications*, *241*, 122697. https://doi.org/10.1016/j.eswa.2023.122697

Kao, D.-Y., & Hsiao, S.-C. (2018). The dynamic analysis of WannaCry ransomware. *2018 20th International Conference on Advanced Communication Technology (ICACT)*. https://doi.org/10.23919/icact.2018.8323682

Karatsareas, P. (2022). Semi-Structured interviews. In R. Kircher & L. Zipp (Eds.), *Research Methods in Language Attitudes* (pp. 99–113). Cambridge University Press.

Kaspersky. (2023, March 16). *Skills gap presents a significant threat to cybersecurity in Africa*. Kaspersky. https://www.kaspersky.co.za/about/press-releases/skills-gap-presents-a-significant-threat-to-cybersecurity-in-africa

Kavak, H., Padilla, J. J., Vernon-Bido, D., Diallo, S. Y., Gore, R., & Shetty, S. (2021). Simulation for cybersecurity: state of the art and future directions. *Journal of Cybersecurity*, *7*(tyab005). https://doi.org/10.1093/cybsec/tyab005

Khan, A., & Malaika, M. (2021). Central Bank Risk Management, Fintech, and Cybersecurity. *IMF Working Papers*, *2021*(105), 1. https://doi.org/10.5089/9781513582344.001

Kianpour, M., Kowalski, S. J., & Øverby, H. (2021). Systematically Understanding Cybersecurity Economics: A Survey. *Sustainability*, *13*(24), 13677. https://doi.org/10.3390/su132413677

KPMG. (2019). *Regulation and supervision of fintech* . https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2019/03/regulation-and-supervision-of-fintech.pdf

Kruger, M., Futcher, L., & Thomson, K.-L. (2022). A Thematic Content Analysis of the Cybersecurity Skills Demand in South Africa. *Human Aspects of Information Security and Assurance*, 24–38. https://doi.org/10.1007/978-3-031-12172-2_3

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

Kuraku, S., Kalla, D., Smith, N., & Samaah, F. (2023). Safeguarding FinTech: Elevating Employee Cybersecurity Awareness In Financial Sector. *International Journal of Applied Information Systems*, *12*(42), 43–47. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4678581

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

Lee, I., & Shin, Y. J. (2018). Fintech: Ecosystem, business models, investment decisions, and challenges. *Business Horizons*, *61*(1), 35–46.

Leszczyna, R. (2021). Review of Cybersecurity Assessment Methods: Applicability Perspective. *Computers & Security*, *108*, 102376. https://doi.org/10.1016/j.cose.2021.102376

Loi, M., & Christen, M. (2020). Ethical Frameworks for Cybersecurity. *The International Library of Ethics, Law and Technology*, *21*, 73–95. https://doi.org/10.1007/978-3-030-29053-5_4

Lombe, M. (2024, October 7). *Security vs Compliance: Understanding the Difference and Why Both Matter In today's world of digital transformation and increasingly complex cyber threats, businesses must not only safeguard their systems but also comply with a wide array of legal and regulatory requirements. While both security and*. Linkedin.com. https://www.linkedin.com/pulse/what-difference-between-security-compliance-muema-fcpzc/

Lucidity Insights. (2023). THE FUTURE OF FINTECH IN AFRICA SPECIAL REPORT 2023. In *Lucidity Insights*. https://elements.visualcapitalist.com/wp-content/uploads/2023/07/FutureFintechAfrica.pdf

Manuel, H., & Thomas , P. (2020). Make Cybersecurity a Strategic Asset - ProQuest. *MIT Sloan Management Review*, *62*(1), 40–45. https://www.proquest.com/docview/2450655586

Marikyan, D., & Papagiannidis, S. (2023). Protection Motivation Theory: A review. In S. Papagiannidis (Ed.), *TheoryHub Book*. https://open.ncl.ac.uk/theory-library/protection-motivation-theory.pdf

McKinsey. (2024, January 16). *What Is Fintech (financial technology)?* Www.mckinsey.com. https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-fintech#/

Mijwil, M., Filali, Y., Aljanabi, M., Bounabi, M., & Al-Shahwani, H. (2023). The Purpose of Cybersecurity Governance in the Digital Transformation of Public Services and Protecting the Digital Environment. *Mesopotamian Journal of Cyber Security*, *2023*, 1–6. https://doi.org/10.58496/mjcs/2023/001

Mishra, A., Alzoubi, Y. I., Gill, A. Q., & Anwar, M. J. (2022). Cybersecurity Enterprises Policies: a Comparative Study. *Sensors*, *22*(2), 538. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8778887/

Mothibi, K., & Lazaridis, D. (2021). FINTECH DIGITAL PLATFORMS – AN INVESTIGATION INTO FINTECH DIGITAL PLATFORM ACTIVITY IN SOUTH AFRICA AND THEIR REGULATORY IMPLICATIONS. In *Financial Services Conduct Authority*. https://www.fsca.co.za/Regulatory%20Frameworks/FinTechDocuments/Fintech_Digital-Platforms_An_investigation_into_Fintech_Digital_platform_activity_in_South_Africa_and_their_regulatory_implications.pdf

Mphatheni, M. R., & Maluleke, W. (2022). Cybersecurity as a response to combating cybercrime. *International Journal of Research in Business and Social Science (2147-4478)*, *11*(4), 384–396. https://doi.org/10.20525/ijrbs.v11i4.1714

Murinde, V., Rizopoulos, E., & Zachariadis, M. (2022). The impact of the FinTech revolution on the future of banking: Opportunities and risks. *International Review of Financial Analysis*, *81*(102103), 102103. Sciencedirect. https://doi.org/10.1016/j.irfa.2022.102103

Najaf, K., Mostafiz, M. I., & Najaf, R. (2021). Fintech firms and banks sustainability: Why cybersecurity risk matters? *International Journal of Financial Engineering*, *8*(2), 2150019. https://doi.org/10.1142/s2424786321500195

Naspers. (2024). *Our Digital Horizon, The Economic Opportunity of Digital Platforms in South Africa*. https://www.naspers.com/~/media/Files/N/Naspers-Corp-V2/digital-horizon-report/full-report-our-digital-horizon-report-the-economic-opportunity-of-digital-platforms-in-south-africa.pdf

Ng, A. W., & Kwok, B. K. B. (2017). Emergence of Fintech and cybersecurity in a global financial centre. *Journal of Financial Regulation and Compliance*, *25*(4), 422–434. https://doi.org/10.1108/jfrc-01-2017-0013

NIST. (2018). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. *Framework for Improving Critical Infrastructure Cybersecurity*, *1.1*(1). https://doi.org/10.6028/nist.cswp.04162018

O'Neill, A. (2024, June 13). *Global gross domestic product (GDP) at current prices from 1985 to 2029*. Statista - The Statistics Portal. Statista. https://www.statista.com/statistics/268750/global-gross-domestic-product-gdp

Odonkor, A. (2020, October 27). *Unveiling the cost of cybercrime in Africa*. News.cgtn.com. https://news.cgtn.com/news/2020-10-27/Unveiling-the-cost-of-cybercrime-in-Africa-UVhmu1PJeM/index.html

Oladipo, J. O., Okoye, C. C., Elufioye, O. A., Falaiye, T., Nwankwo, E. E., Oladipo, J. O., Okoye, C. C., Elufioye, O. A., Falaiye, T., & Nwankwo, E. E. (2024). Human factors in cybersecurity: Navigating the fintech landscape. *International Journal of Science and Research Archive*, *11*(1), 1959–1967. https://doi.org/10.30574/ijsra.2024.11.1.0258

Payments Association of South Africa. (2023, May 5). *Key Role-Players - Payment Association of South Africa (PASA)*. Pasa.org.za. https://pasa.org.za/national-payment-system/key-role-players/

Pieterse, H. (2021). The Cyber Threat Landscape in South Africa: A 10-Year Review. *The African Journal of Information and Communication*, *28*(28). https://doi.org/10.23962/10539/32213

Puschmann, T. (2017). Fintech. *Business & Information Systems Engineering*, *59*(1), 69–76. https://doi.org/10.1007/s12599-017-0464-6

Ramluckan, T., van Niekerk, B., & Leenen, L. (2020). Cybersecurity and Information Warfare Research in South Africa: Challenges and Proposed Solutions. *Journal of Information Warfare*, *19*(1), 80–95. https://www.jstor.org/stable/27033610

Ramoabi, N. (2021). *Banking on Technology for Better Access: An evaluation of the law regulating fintech and credit scoring in South Africa* [Masters' thesis]. https://arno.uvt.nl/show.cgi?fid=155525

Ramona, E. (2011). Advantages and disadvantages of quantitative and qualitative information risk approaches. *Chinese Business Review*, *10*(12), 1106–1110. https://www.davidpublisher.com/Public/uploads/Contribute/555d6fdde07cc.pdf

Raphoto, K. (2021). *Fintech Start-ups in South Africa - A conceptual framework to guide technology entrepreneurs* [MCom Thesis]. https://repository.up.ac.za/bitstream/handle/2263/78920/Raphoto_Fintech_2021.pdf?sequence=3

Rashidi, M., Begum, R., Mokhtar, M., & Pereira, J. (2014). The Conduct of Structured Interviews as Research Implementation Method . *Journal of Advanced Research Design ISSN*, *1*(1), 28–34. https://www.akademiabaru.com/doc/ARDV1_N1_P28_34.pdf

Restoy, F. (2020). *Regulating fintech: what is going on, and where are the challenges?* https://www.suerf.org/publications/suerf-policy-notes-and-briefs/regulating-fintech-what-is-going-on-and-where-are-the-challenges/

Salah AlBenJasim, Tooska Dargahi, Haifa Takruri, & Rabab Al-Zaidi. (2023). FinTech Cybersecurity Challenges and Regulations: Bahrain Case Study. *Journal of Computer Information Systems*, 1–17. https://doi.org/10.1080/08874417.2023.2251455

Sarker, I. H. (2022). Machine Learning for Intelligent Data Analysis and Automation in Cybersecurity: Current and Future Prospects. *Annals of Data Science*, *10*, 1473–1498. https://doi.org/10.1007/s40745-022-00444-2

Sarker, I. H., Furhad, M. H., & Nowrozy, R. (2021). AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions. *SN Computer Science*, *2*(3). https://doi.org/10.1007/s42979-021-00557-0

Saunders, M., Lewis, P., & Thornhill, A. (2023). *Research Methods for Business Students* (9th ed.). Pearson. (Original work published 1997)

Șcheau, M. C., Călin, M. R., Popescu, F. V., & Leu, D. M. (2022). Key Pillars for FinTech and Cybersecurity. *Acta Universitatis Danubius. Œconomica*, *18*(1). https://www.proquest.com/docview/2769349027?pq-origsite=gscholar&fromopenview=true&sourcetype=Scholarly%20Journals

Schiliro, F. (2022). *Towards a Contemporary Definition of Cybersecurity*. https://arxiv.org/pdf/2302.02274

Schlehahn, E. (2020). Cybersecurity and the State. *The International Library of Ethics, Law and Technology*, *21*, 205–225. https://doi.org/10.1007/978-3-030-29053-5_10

Schroeder, K., Trinh, H., & Pillitteri, V. (2021). *Measurement Guide for Information Security: Volume 1 — Identifying and Selecting Measures*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-55v1.ipd

Schueffel, P. (2016). Taming the Beast: A Scientific Definition of Fintech. *SSRN Electronic Journal*, *4*(4), 32–54. https://doi.org/10.2139/ssrn.3097312

Shaukat, K., Luo, S., Varadharajan, V., Hameed, I. A., Chen, S., Liu, D., & Li, J. (2020). Performance Comparison and Current Challenges of Using Machine Learning Techniques in Cybersecurity. *Energies*, *13*(10), 2509. https://doi.org/10.3390/en13102509

Slazus, B. J., & Bick, G. (2022). *Factors that influence FinTech adoption in South Africa : a study of consumer behaviour towards branchless mobile banking*. Www.zbw.eu. http://hdl.handle.net/11159/6590

South African Banking Risk Information Centre. (2023). *SABRIC Crime Statistics 2022 2022 Annual Crime Statistics SABRIC Crime Statistics 2022*. https://www.sabric.co.za/media/gq4hmbjw/sabric-annual-crime-stats-2022.pdf

South African Reserve Bank. (2024). *Digital Payments Roadmap: Towards inclusive, accessible, effective and sustainable digital payments in South Africa*. https://www.resbank.co.za/content/dam/sarb/publications/media-releases/2024/npsd---payments-report/Digital%20Payments%20Roadmap%20Report.pdf

Sutherland, E. (2017). Governance of Cybersecurity – The Case of South Africa. *The African Journal of Information and Communication*, *20*(20), 83–112. https://doi.org/10.23962/10539/23574

Świątkowska, J. (2020). *Tackling cybercrime to unleash developing countries' digital potential*. https://api.semanticscholar.org/CorpusID:235665245

Teoh, C. S., Kamil Mahmood, A., & Dzazali, S. (2018, August 1). *Cyber Security Challenges in Organisations: A Case Study in Malaysia*. IEEE Xplore. https://doi.org/10.1109/ICCOINS.2018.8510569

Tsakalidis, G., & Vergidis, K. (2019). A Systematic Approach Toward Description and Classification of Cybercrime Incidents. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, *49*(4), 710–729. https://doi.org/10.1109/tsmc.2017.2700495

Watson, R., & Bergman, R. (2023, October 1). *Cybersecurity Leadership Insights: mastering complexity*. Www.ey.com. https://www.ey.com/en_gl/insights/consulting/is-your-greatest-risk-the-complexity-of-your-cyber-strategy

Werth, O., Torno, A., Breitner, M. H., Muntermann, J., & Cardona, D. R. (2023). What determines FinTech success?—A taxonomy-based analysis of FinTech success factors. *Electronic Markets*, *33*(1). https://doi.org/10.1007/s12525-023-00626-7

Williamson, I. (2024, March 27). The Money Show (B. Whitfield, Interviewer) [Interview]. In *Primedia*. https://www.primediaplus.com/ceo-of-old-mutual-earnings-rise-on-strong-new-business-flows-mpc-decides-to-keep-rates-unchanged-at-825/

World Economic Forum. (2023). *The Global Risks Report 2023 (18th ed.)*. https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf

Appendix A — Research instrument

Introduction

- Greetings and thanks for participation.
- Brief explanation of research (evaluating cybersecurity governance in SA fintechs).
- Outline the three parts of the interview.
- Expected interview duration (45 to 60 minutes).
- Assurance of confidentiality and anonymity.
- Request permission to record and transcribe.

Questions

Part 1 — Business context questions:

- Briefly describe your company and its primary products as they relate to fintech.
- How long has the company been in operation?
- How many employees are in your company ?
- Briefly describe your role and responsibilities in the cybersecurity function.
- How many years of experience do you have in cybersecurity and in your current role?

Part 2 — Core interview questions:

Governance:

- Do you have other responsibilities outside of cybersecurity?
- What is the main contributor to your KPIs (e.g., compliance, incidents, etc)?
- Do you have a formal security policy that is accepted across the business?
- Does cybersecurity have executive sponsorship, and what is the governance structure?
- Is there alignment between the organisational and cybersecurity goals?
- What are the challenges or gaps within the governance framework?

Operations:

- How many people are dedicated to the cybersecurity function?
- Are cybersecurity processes and procedures formally documented and distributed?
- Are there any challenges in terms of capacity or skills within the cybersecurity team?
- What is the level of automation in terms of detecting, and responding to incidents?
- What is the level of collaboration / process integration between cybersecurity and other departments?

- How are you leveraging artificial intelligence, blockchain, cloud, and big data technologies within the cybersecurity function?
- What are the challenges in your cybersecurity operations?

Planning:

- How are cybersecurity requirements integrated into overall business strategy?
- What are the challenges experienced during planning for cybersecurity initiatives?

Risk management:

- How are cybersecurity risks monitored and prioritised?
- How are cybersecurity risks communicated to top management?
- What are the challenges in cybersecurity risk management?

Project support:

- Are cybersecurity requirements integrated into project management processes?
- What is the overhead introduced by cybersecurity in project delivery?
- What are the challenges encountered in providing cybersecurity support for projects?

Part 3 — Additional insights:

- What support or resources would be most helpful in improving cybersecurity governance in your company?
- What are the most significant cybersecurity challenges specific to fintechs in South Africa?
- How do you see the future of cybersecurity in the South African fintech sector?

Closing

- Thank you for participation and valuable insights.
- Opportunity for interviewee to ask questions.
- Reminder of confidentiality and anonymity.

Appendix B — Research participation consent form

Title of project: Evaluating cybersecurity governance challenges in South African fintechs

Name of researcher: Norman Nhliziyo

I, ……., agree to participate in this research project.

I agree to the following:

(Please circle the relevant options below)

The research study was explained to me. I understand what this study is about.	YES	NO
I understand that I can volunteer to take part in the study.	YES	NO
I agree that the interview activity may be video recorded and transcribed.	YES	NO
I agree that direct quotations from my interview may be used by the researcher in his research report.	YES	NO
I agree that my participation will remain anonymous (my name or other identifying data will not be used by the researcher in his research report	YES	NO
I agree that other researchers may use the information I provide in my interview (depending on their own ethics clearance being obtained) subject to my name and any other personal information not being used or passed on.	YES	NO

…… (signature)

…… (name of participant)

…… (date)

…… (signature)

…… (name of researcher/person seeking consent)

…… (date)

Appendix C — Research submission checklist

UNIVERSITY OF THE WITWATERSRAND, JOHANNESBURG

WITS FACULTY OF COMMERCE, LAW & MANAGEMENT

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

**** This checklist must be completed and included as part of the submission. ****

Name of candidate:	Norman Nhliziyo	
Person / student number:	2696297	
Qualification:	Master of Business Administration	
Title:	Evaluating cybersecurity governance challenges in South African fintechs	
Supervisor(s):	Dr. Sylvester Horvey	
Contact details:	**Cell number(s):** 0715847287	**Email:** 2696297@students.wits.ac.za

FIRST SUBMISSION CHECKLIST *(for Examination)*

Has this research been submitted with the consent of the supervisor? (Y/N)		Y
Student to submit:	**Electronic copy of research in PDF** *(Hard copy may be required upon request from the examiner)*	Y
	Full Turn-it-in report *(signed by Supervisor)* *** For WBS – this report does not require the Supervisor's approval ***	Y
	Confirmation of ethics (*Clearance/Waiver certificate*)	Y
	Overall supervisor evaluation form *(MBA candidates ONLY)*	Y
Supervisor to submit:	**University clearance certificate** *(Supervisor to complete and send directly to Faculty)*	N/A
	Supervisor's report *(Supervisor to complete and send directly to Faculty)*	N/A
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:

- *Incomplete submissions will NOT be prioritised.*
- *Outstanding fees must be cleared to enable Awaiting Examiner's registration (upon submission).*
- *WBS submissions may undergo internal academic quality checks before the exam process may begin.*
- *There may be a delay in the examination process – for more information, click:* **Exam Process**
- *For more information on the graduation, click:* **Graduation info.** and **Graduations Office**

Annexure A — Research approval

UNIVERSITY OF THE WITWATERSRAND, JOHANNESBURG

Private Bag 3 Wits, 2050
Fax:
Tel:

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

02 July 2024
Person No: 2696297
PAG

Mr NWGK Nhliziyo
239 Sagewood Lifestyle Estates
Cnr Olifantsfontein & Lever Road
Country View
1687
South Africa

Dear Mr Norman Nhliziyo

Master of Business Administration: Approval of Title

We have pleasure in advising that your proposal entitled *Evaluating cybersecurity governance challenges in South African fintechs* 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 B — Ethics clearance certificate

Graduate School of Business Administration
University of the Witwatersrand, Johannesburg

Wits Business School

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

Ethics Clearance Certificate

Ethics protocol number: WBS/BA2696297/409
This certificate is only valid with a legitimate ethics protocol number and signed by the Researcher (below).

Project title	Evaluating cybersecurity governance challenges in South African fintechs
Investigator / Researcher	Mr Norman Nhliziyo
Nature of Project	MBA (Research Article)
Decision of the Committee	Approved, provided stakeholders and participants are guaranteed confidentialty.
Issue Date of Certificate	04/07/2024
Expiry date	Date of submission of the project / research report
Chairperson	Dr Ayanda Magida ☎ +27 11 717 3953 ✉ ayanda.magida@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.

Signature

2024-07-08
Date:

Annexure C — Turnitin originality report

Processed on: 25-Feb-2025 10:33 AM SAST
ID: 2598206977
Word Count: 8440
Submitted: 1

Evaluating cybersecurity governance challenge... By Norman Nhliziyo

Similarity Index	Similarity by Source	
7%	Internet Sources:	7%
	Publications:	2%
	Student Papers:	N/A

This receipt acknowledges that Turnitin received your paper. Below you will find the receipt information regarding your submission.

The first page of your submissions is displayed below.

Submission author:	Norman Nhliziyo
Assignment title:	Final Report Submission Link
Submission title:	Evaluating cybersecurity governance challenges in South Afric...
File name:	Evaluating_cybersecurity_governance_challenges_in_South_Afr...
File size:	509.45K
Page count:	29
Word count:	8,440
Character count:	50,295
Submission date:	25-Feb-2025 10:33AM (UTC+0200)
Submission ID:	2598206977