

https://dspace.org/

Cybersecurity Perspectives on Protecting Intangible Commodities in the South African Financial Sector

Naidoo, Trevor

2024
University of the Witwatersrand, Johannesburg
https://hdl.handle.net/10539/43974
Naidoo, Trevor. (2024). Cybersecurity Perspectives on Protecting Intangible Commodities in the South African Financial Sector [Master's dissertation, University of the Witwatersrand, Johannesburg].WireDSpace.

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

Cybersecurity Perspectives on Protecting Intangible Commodities in the South African Financial Sector

Trevor Naidoo

851470

851470@students.wits.ac.za, +27 71 495 7620

Supervisor: Prof. Nixon Ochara

Nixon.ochara@wits.ac.za, +27 72 170 4560

A dissertation 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 Management in the field of Digital Business

Johannesburg, 2024

ABSTRACT

The reliance on digital technologies in the financial industry has surged, elevating the value of intangible commodities like data and intellectual property. South Africa's financial sector faces escalating cyber threats, necessitating robust cybersecurity measures. This quantitative research aims to explore cybersecurity perspectives in safeguarding intangible assets within South African financial institutions.

The importance of cybersecurity in safeguarding individuals and organisations from cyber threats is underscored, considering the significant financial losses and reputational damage that can result from breaches. However, challenges such as workforce shortages, skills gaps, and a lack of cybersecurity awareness persist, particularly among SMEs. The theoretical framework provides insights into individual and organisational behaviour regarding cybersecurity practices.

The dissertation aimed to gather insights from technology professionals and influential leaders in cybersecurity within the financial sector of South Africa. Valuable insights into the factors influencing cybersecurity attitudes and behaviours in the South African financial sector, emphasising the importance of enforceability, subjective norms, and violation coupling in shaping attitudes towards behaviour.

The study delves into key controls, monitoring effectiveness, and the feasibility of adopting global standards. By providing insights and recommendations, this research contributes to enhancing cybersecurity in South Africa's financial sector, crucial for maintaining trust, compliance, and stability in an increasingly digital world.

KEYWORDS

Cybersecurity, Cyberspace, Intangible commodities, Financial Institutions, South Africa, Risk Mitigation

DECLARATION

I, Trevor Naidoo, declare that this research report is my own work except as indicated in the references and acknowledgements. It is submitted in partial fulfilments of the requirements for the degree of Master of Management in the field of Digital Business 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: Trevor Naidoo

Signature: Trevor Naidoo

Signed at Centurion

On the 27 May 2024

ACKNOWLEDGEMENTS

I extend heartfelt gratitude to the individuals who played pivotal roles in making this study a reality:

First and foremost, I am deeply thankful to my parents, who instilled in me the value of education from a tender age. Their unwavering support laid the foundation for my academic pursuits.

A special acknowledgment goes to my beloved wife, Kathleen, and our daughter, Alayna. Their boundless love, patience, and understanding have sustained me throughout the past two years of this journey. Despite the countless hours I dedicated to this endeavour, they never wavered in their support. Kathleen and Alayna, you are my pride and joy, and I am immensely grateful for your unwavering patience. May my dedication inspire you both to pursue your own educational dreams as you continue to grow.

I am indebted to my circle of friends, colleagues, and acquaintances whose encouragement and motivation served as constant sources of inspiration. Their unwavering belief in me kept me going, even during the most challenging moments.

I express sincere appreciation to my manager, Nomusa Mosima, whose encouragement and unwavering support helped me stay focused on my academic pursuits. Nomusa's active interest in my learning journey served as a constant source of motivation.

Last but not least, I am profoundly grateful to my supervisor, Prof. Nixon Ochara. His guidance, motivation, and support were instrumental throughout this process. The invaluable advice I received from Prof. Ochara will continue to guide me as I embark on my journey towards a Ph.D.

TABLE OF CONTENTS

DECLARATION iii

ACKNOWLEDGEMENTS iv

TABLE OF CONTENTS v

LIST OF TABLES ix

LIST OF FIGURES xi

LIST OF ACRONYMS xii

CHAPTER 1. INTRODUCTION 13

1.1 STATEMENT OF PURPOSE 13
1.2 BACKGROUND OF THE STUDY 13
1.3 FINANCIAL SYSTEM 15
1.3.1 SOUTH AFRICAN FINANCIAL SECTOR 16
1.3.2 CYBERSECURITY IN SOUTH AFRICA 17
1.4 RESEARCH PROBLEM 18
1.5 RESEARCH OBJECTIVES 20
1.5.1 RESEARCH QUESTIONS 20
1.6 RATIONALE 21
1.7 DELIMITATIONS OF THE STUDY 22
1.8 DEFINITION OF TERMS 22
1.9 ASSUMPTIONS 24
1.10 CHAPTER OUTLINE 25
1.11 CONCLUSION 26

CHAPTER 2. LITERATURE REVIEW AND THEORETICAL FRAMEWORK. 27

2.1 INTRODUCTION 27
2.2 CYBERSPACE 27
2.2.1 VIRTUAL LAYER 28
2.2.2 LOGICAL LAYER 29
2.2.3 PHYSICAL LAYER 29

2.3 CYBERSECURITY 30
2.3.1 IMPORTANCE OF CYBERSECURITY 31
2.3.2 CHALLENGES OF CYBERSECURITY 32
2.3.3 BEST PRACTICES FOR CYBERSECURITY 33
2.4 ANALYTICAL FRAMEWORK 37
2.4.1 THEORETICAL FRAMEWORK 37
2.4.2 CONCEPTUAL FRAMEWORK 40
2.5 HYPOTHESIS 42
2.6 CONCLUSION OF LITERATURE REVIEW 45

CHAPTER 3. RESEARCH METHODOLOGY 47

3.1 RESEARCH APPROACH 47
3.2 RESEARCH PARADIGM 47
3.3 RESEARCH DESIGN 48
3.4 DATA COLLECTION METHOD 49
3.5 POPULATION AND SAMPLE 49
3.5.1 POPULATION 49
3.5.2 SAMPLE AND SAMPLING METHOD 50
3.6 RESEARCH INSTRUMENT 53
3.7 DATA ANALYSIS AND INTERPRETATION 54
3.8 RELIABILITY AND VALIDITY 54
3.8.1 RELIABILITY 55
3.8.2 VALIDITY 55
3.9 LIMITATIONS OF THE STUDY 56
3.10 ETHICAL CONSIDERATIONS 56

CHAPTER 4. PRESENTATION OF RESULTS 58

4.1 INTRODUCTION 58
4.2 DEMOGRAPHIC ANALYSIS 58
4.3 DESCRIPTIVE ANALYSIS 59
4.3.1 RELIABILITY AND VALIDITY ANALYSIS 59
4.3.2 VIOLATION COUPLING 62
4.3.3 COMMUNICATION STRUCTURES 62
4.3.4 RULES CONNECTEDNESS 62
4.3.5 ENFORCEABILITY 63
4.3.6 GOAL CLARITY OF RULES 63
4.3.7 ATTITUDE TOWARDS BEHAVIOUR 63
4.3.8 SUBJECTIVE NORMS 63
4.4 FACTOR ANALYSIS 63
4.4.1 COMMUNICATION STRUCTURES 65
4.4.2 ENFORCEABILITY 65

4.4.3 Goal Clarity of Rules 66
4.4.4 Attitude towards Behaviour 66
4.4.5 Rule Connectedness 66
4.4.6 Subjective Norms 66
4.4.7 Violation Coupling 67
4.5 Hypothesis Testing 67
4.6 Regression Analysis 73
4.7 Conclusion 76

CHAPTER 5. INTEPRETATION OF THE RESULTS 79

5.1 Introduction 79
5.2 Hypothesis Summary Results 79
5.2.1 The perceived risk of violating a privacy or cybersecurity rule negatively affects the likelihood of a privacy or security rule violation aimed at safeguarding intangible commodities 79
5.2.2 Instances of violations linked to negative outcomes will increase the perception of risk associated with rule violation for individuals and organisations. 80
5.2.3 Connectedness (referring to network connections or relationships) will positively influence the perception of risk of violating rules for individuals and organisations. 81
5.2.4 Subjective norms will positively influence the perception of risk of violating rules for individuals. 81
5.2.5 Both formal and informal communication structures that promote regulatory compliance will heighten the perception of risk regarding rule violation for individuals and organisations. 82
5.2.6 The enforceability of regulations will positively impact the perception of risk of rule violation for individuals and organisations. 83
5.2.7 A positive attitude towards rule-abiding behaviour will positively influence the perception of risk of violating rules for individuals and organisations. 83
5.2.8 The clarity of goals in rules and regulations will positively influence the perception of risk of violating those rules for individuals and organisations. 84
5.3 Conclusion 84
5.3.1 Identify the key cybersecurity controls relevant to protecting intangible commodities 84
5.3.2 Evaluate the feasibility and viability of adopting global frameworks and standards in the context of South Africa's connected world. 85
5.3.3 Develop a monitoring and measurement framework to assess the effectiveness of current cybersecurity controls for safeguarding intangible commodities 86

CHAPTER 6. CONCLUSION AND RECOMMENDATIONS 88

6.1 Introduction 88
6.2 Conclusion 88
6.2.1 Identify the key cybersecurity controls relevant to protecting intangible commodities 89
6.2.2 Evaluate the feasibility and viability of adopting global frameworks and standards in the context of South Africa's connected world. 90
6.2.3 Develop a monitoring and measurement framework to assess the effectiveness of current cybersecurity controls for safeguarding intangible commodities 91
6.3 Recommendations 92
6.3.1 Practice 92

6.3.2 THEORETICAL CONTRIBUTIONS 93
6.4 LIMITATIONS OF THE STUDY 93
6.5 RECOMMENDATIONS FOR FUTURE STUDIES 94

REFERENCES 96

Appendix A: Data-Collection Instrument 113

Appendix B: Survey Participation Request 120

Appendix C: Ethics Clearance Certificate 122

LIST OF TABLES

Table 1. List of Acronyms xii

Table 2. Manual Database of Financial Institutions 50

Table 3. Target Criteria 51

Table 4. Target Sample Size 52

Table 5. Likert 5-point scale used 53

Table 6. Demographic Analysis 59

Table 7. Construct Reliability and Validity Overview 60

Table 8. Descriptive statistics 61

Table 9. Indicator Data 65

Table 10. VIF Values in the Structural Model 69

Table 11. Path Coefficients 70

Table 12. Percentile Confidence Intervals (with Bias Correction) for the Path Coefficients 70

Table 13. R squared 71

Table 14. F Effect Sizes 71

Table 15. PLSpredict Results Report 72

Table 16. Total Effects 73

Table 17. ANOVA..... 74

Table 18. Coefficients..... 76

Table 19. Summary of Hypothesis and Results..... 78

LIST OF FIGURES

Figure 1. Total Malware (Source: av-test-org) 14

Figure 2. The financial system (Brigit Helms, 2006) 16

Figure 3. Three Lines of Defence Model (Source: University of Mississippi) 19

Figure 4. Virtual Layer (*National Cyber Strategy*, 2022) 28

Figure 5. Logical Layer (*National Cyber Strategy*, 2022) 28

Figure 6. Physical Layer (*National Cyber Strategy*, 2022) 29

Figure 7. 8 Steps of Data Management Lifecycle (Tim Stobierski, 2021) 30

Figure 8. SABRIC Scam and Fraud Activity (Source: Sabric) 31

Figure 9. Word Cloud of Industry Certification Listings 33

Figure 10. Theory of Reasoned Action (Thomas Sarver Jr., 1983) 39

Figure 11. Overview of the selective organisational information privacy and security violations model (SOIPSVM), (Source: (Wall et al., 2015)) 41

Figure 12. Bootstrapping p values in the Modelling Window 69

Figure 13. Importance Performance Map Analysis (IPMA) 72

LIST OF ACRONYMS

Acronym	Meaning
PII	Personal Identifiable Information
ICT	Information And Communication Technologies
GDP	Gross Domestic Product
SAPS	South African Police Service
NPA	National Prosecuting Authority
NCPF	National Cybersecurity Policy Framework
ERMF	Enterprise Risk Management Framework
ROSI	Return On Security Investment
AI	Artificial Intelligence
SABRIC	South African Banking Risk Information Centre
SME	Small And Medium-Sized Enterprises
ISMS	Information Security Management System
CIS	Center For Internet Security
COBIT	Control Objectives For Information And Related Technologies
ISACA	Information Systems Audit And Control Association
ITGI	It Governance Institute
NIST	National Institute Of Standards And Technology
CSF	Cybersecurity Framework
SOIPSVM	Selective Organisational Information Privacy And Security Violations Model
GST	General Strain Theory
TRA	Theory Of Reasoned Action
SOVRM	Selective Organisational Rule Violations Model
INT	Institutional Theory
RDT	Resource Dependence Theory

Table 1. List of Acronyms

CHAPTER 1. INTRODUCTION

1.1 Statement of purpose

Reliance on digital technologies is increasing daily, and the value of intangible commodities such as data, intellectual property, and customer information has grown exponentially. In the financial industry, these intangible commodities are especially valuable as they form the basis of financial transactions and relationships. However, financial institutions are also prime targets for cyber-attacks, and protecting these intangible commodities has become crucial for safeguarding the privacy and confidentiality of customer data, ensuring regulatory compliance, and maintaining the reputation of financial institutions.

South Africa's financial industry is no exception, and cybersecurity has become a top priority for financial institutions. In recent years, South Africa has seen a surge in cybercrime, with high-profile data breaches and cyber-attacks targeting financial institutions. Protecting intangible commodities has become challenging for financial institutions, and they must adopt a multifaceted approach to address the evolving cyber threats.

The digital evolution transforming financial institutions at a rapid pace requires effort in ensuring personal and financial information stays safe. This quantitative research aims to provide a comprehensive overview of cybersecurity perspectives for protecting intangible commodities in financial institutions within South Africa.

1.2 Background of the study

As outlined by the researchers Jang-Jaccard and Nepal (2014), society, critical infrastructure and economies have become dependent on information technology solutions (Jang-Jaccard & Nepal, 2014). This dependency on technology adds to the

positive Gross Domestic Product (GDP) growth and increased social development of countries. However, as Information and Communication Technologies (ICT) advance and develop, individuals and organisations are susceptible to Cyber-attacks which have grown exponentially (Figure 1.). Governments, Organisations and individuals have growing concerns about cybersecurity and the protection of data integrity and data confidentiality and safe access to cyberspace (Bahiti & Josifi, 2015). Demek and Kaplan (2023), supported these concerns and expanded the parties to Investors, managers, customers and the public (Demek & Kaplan, 2023).

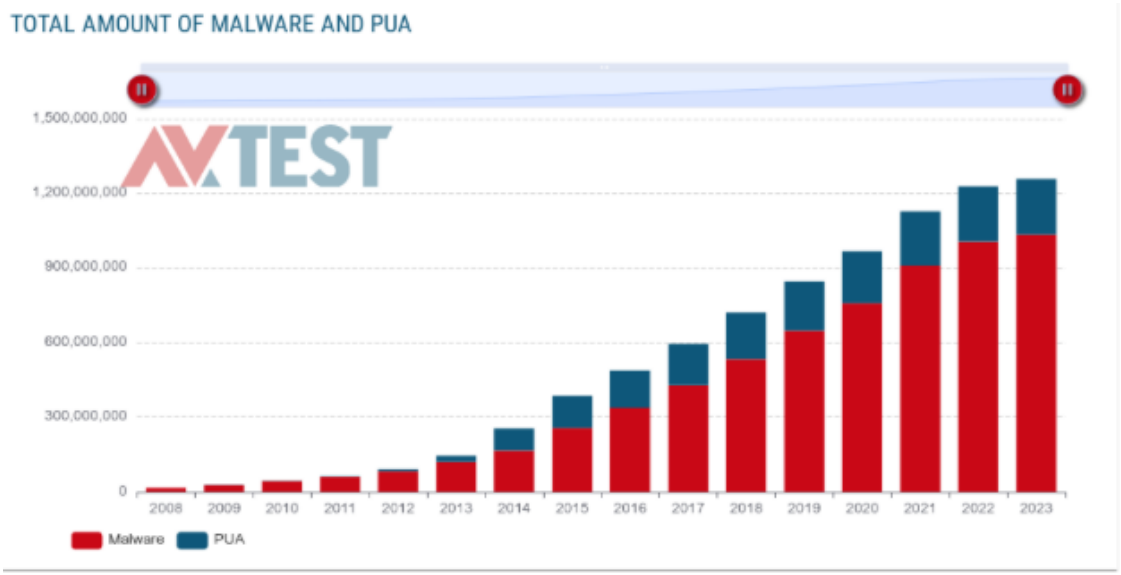


Figure 1. Total Malware (Source: av-test-org)

Bahiti and Josifi (2015), went on to further state while the internet is a common resource, security is a shared responsibility. Everyone has a role in securing their part of Cyberspace (Bahiti & Josifi, 2015). Goutam (2015), defines cybersecurity as technologies and processes constructed to protect digital hardware and software from unauthorised access, vulnerabilities or hackers (Goutam, 2015). Cyber-attacks can severely damage all sectors of economies with notable financial loss and disruption of vital services (Bahiti & Josifi, 2015).

Globally financial institutions have been faced with increasing cyber-attacks. JPMorgan Chase was targeted in a cyber data breach which resulted in 76 million households and 7 million small business information being leaked (Glazer & Yadron, 2014). Capital One also suffered an intrusion and loss of personal information in July 2019 that impacted 100 million customers in the United States and 6 million in Canada (Novaes Neto et al., 2020). TransUnion South Africa was attacked by N4aughtysecTU, a hacking group that obtained an undisclosed amount of names and ID numbers (Moyo, 2022). Experian confirmed a breach which resulted in circa 24 million personal information records stolen and 793 749 business entities' information records which was infiltrated (Muncaster, 2020).

The severity of information exposed through these data breaches allows for further crimes to be committed such as identity theft, ransomware attacks, malware injections and larger organised crimes such as Terrorism, sabotage and possibly information warfare. These breaches are all unique and have advanced sophisticated means which have been used to circumvent security controls.

The study aims to provide insights into the cybersecurity controls, measures and strategies that financial institutions in South Africa have put in place to protect their intangible assets. It further examines the challenges faced by these institutions in protecting their intangible assets as emerging technologies are adopted.

1.3 Financial System

Helms described a financial system (figure 2.) as an integrated system which a client interacts across three levels, Micro, Meso and Macro levels (Brigit Helms, 2006). The micro level is distinct as clients interact with the institutions directly, the financial service providers. Each one providing unique or similar product or services that derive value for the client and in return the entity earns income from selling their services and products.

The meso level considers the infrastructure where clients can access services and products. Simultaneously support services enhance the offerings by financial service providers by holding them responsible and ensuring services are not compromised. Auditors, credit bureaus, Information technology, telecoms and rating agencies are examples. The macro level are the regulatory bodies that define legislations, policies and frameworks that are design to ensure financial institutions and market infrastructures operate within the South African financial system are inherently safe and sound for its citizens.



Figure 2. The financial system (Brigit Helms, 2006)

1.3.1 *South African Financial Sector*

The financial sector in South Africa plays a crucial role in the country's economy, as it contributes significantly to employment, investment, and GDP growth. The sector comprises various institutions, including commercial banks, insurance companies, asset management firms, and pension funds. These institutions are regulated by the South African Reserve Bank, which is responsible for maintaining financial stability and supervising the financial sector.

According to the World Bank, South Africa's financial sector has undergone significant changes and reforms in recent years, which have helped to increase access to financial services and improve the sector's efficiency and stability (Elliott & Verkoren, 2022).

One of the notable changes in the financial sector is the adoption of digital technologies and mobile banking. This has helped to reach underserved populations and improve financial inclusion (*6 Challenges to Financial Inclusion in South Africa*, 2017).

The financial sector has also been impacted by the COVID-19 pandemic, which has led to increased uncertainty and financial stress for many households and businesses (Bagui et al., 2023). However, the sector has responded with various measures, such as loan payment holidays, debt restructuring, and increased lending to support businesses and households (Mukherjee, 2020).

1.3.2 *Cybersecurity in South Africa*

Cabinet adopted a National Cybersecurity Policy Framework (NCPF) for South Africa on 7th March 2012. Within the NCPF the purpose is highlighted 'to create a secure, dependable, reliable and trustworthy cyber environment that facilitates the protection of critical information infrastructure whilst strengthening shared human values and understanding of Cybersecurity in support of national security imperatives and the economy' (Mahlobo, 2015). This initiative was driven by the principles of an information society, which uphold the essential rights of all South African citizens, including privacy, security, dignity, access to information, communication rights, and freedom of expression. These rights are safeguarded to ensure individuals can fully enjoy the advantages of a safe and secure online environment. (Ewan Sutherland, 2017).

South Africa has been flagged as the country with the most cyber-attacks in Africa (Van Heerden et al., 2016); (Modise, 2023), with an estimated annual cost of ZAR 2.2 billion (Modise, 2023). Industry reports on cybersecurity point to realities as experienced by consumers and firms but rather offer more specific information about their products

and services to address these realities. Businesses face legal liability for the loss of customer data and the consequential fall in share prices, reputational damage and deterioration of customer loyalty. In South Africa, we assume the cost is not entirely true and reported lower than what it truly is as not all cyber incidents are reported and as such, the South African Police Service (SAPS) or the National Prosecuting Authority (NPA) offers no resources or statistics (Pieterse, 2021).

1.4 Research problem

Organisations are expanding efforts to collect and use customer data to increase profits and market share (Martin et al., 2017). Data's effect on business is pervasive through four main factors as observed by the World Economic Forum (WEF), customer expectations, product enhancement, collaborative innovation, and organisational forms (Klaus Schwab, 2016). This has led to growing concerns about stored customer data and has directed various regulations and policies globally that are focused on the privacy and protection of Personal Identifiable Information (PII). Government should not only protect user privacy and personal information but also seek to derive value from the information (Yang et al., 2019).

This is supported by Walton et al. (2021), who suggested with an increase in the retention of customer data, cyber breaches increase (Walton et al., 2021). Simultaneously as the world increases digitalisation, so will the vulnerabilities increase across the tight-knit financial and technologically interconnected industry (Tobias Adrian & Caio Ferreira, 2023).

In a digital world to mitigate these threats, organisations need to understand the risk exposure and define their appetite in accordance with the Enterprise Risk Management Framework (ERMF). The three lines of defence exist within the ERMF to ensure the exposure is limited and the compensating controls are in place to prevent any malicious intent (Amelia Ho, 2018).

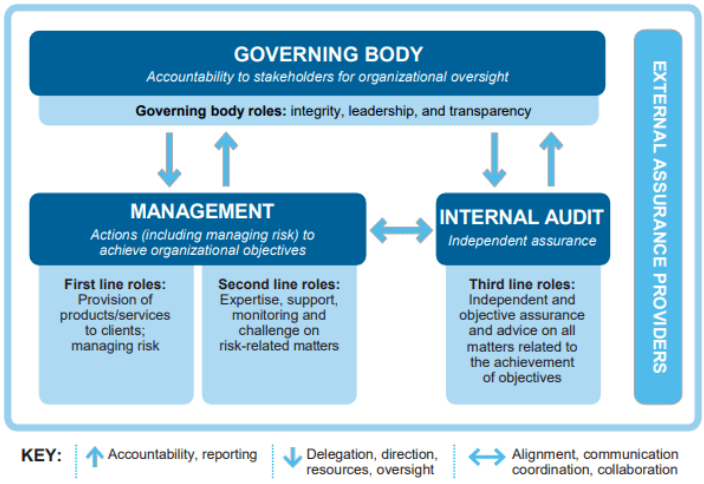


Figure 3. Three Lines of Defence Model (Source: University of Mississippi)

Each layer function as an organisation's end-to-end defence model as depicted in Figure 3. The model starts at the operational level up the hierarchy to risk and compliance units and ultimately to internal audit which facilitate the assurance of the effectiveness of designs (Amelia Ho, 2018).

The author (Maalem Lahcen et al., 2020) states security is a secondary task for users when it's not their primary job function. System developers prioritise users' needs before incorporating security as part of the architectural design. In the era of digitalisation, today's data storage is available on the cloud rather than paper (Singh et al., 2021). As noted from the case study done on Capital One, organisations are faced with urgency to understand the threats that can expose their data as well as the need to understand and comply with the emerging regulations and laws involving data protection within their countries for their business operations (Novaes Neto et al., 2020).

Ensuring the security of intangible commodities requires a robust set of cybersecurity controls tailored to the digital landscape. Key controls include encryption protocols, access controls, regular vulnerability assessments, and incident response plans. Monitoring the effectiveness of these controls is crucial, employing metrics such as incident response times, detection rates, and compliance with regulatory standards.

Continuous evaluation and adjustment are essential to stay ahead of evolving threats. As for South Africa, the feasibility of adopting global frameworks and standards in a connected world hinges on various factors such as infrastructure readiness, regulatory alignment, and stakeholder collaboration. While integration offers benefits like enhanced interoperability and alignment with international best practices, local nuances and resource constraints must be considered to ensure effective implementation and sustainability.

1.5 Research objectives

The research aims to provide a comprehensive overview of cybersecurity perspectives for protecting intangible commodities in financial institutions in South Africa. The specific objectives are:

1. Identify the key cybersecurity controls relevant to protecting intangible commodities.
2. Develop a monitoring and measurement framework to assess the effectiveness of current cybersecurity controls for safeguarding intangible commodities.
3. Evaluate the feasibility and viability of adopting global frameworks and standards in the context of South Africa's connected world.

To provide recommendations for improving cybersecurity in financial institutions in South Africa.

1.5.1 *Research Questions*

Investigate and understand how financial institutions in South Africa are limited when protecting intangible commodities.

1. What are the key cybersecurity controls for protecting intangible commodities?
2. How to monitor and measures the effectiveness of current cybersecurity controls for protecting intangible commodities?

3. Is the adoption of global frameworks and standards operating in a connected world viable and or feasible for South Africa?

1.6 Rationale

Existing studies demonstrate that financial services allocate a minimum of 10% budget to cybersecurity. This element is heavily reliant on expensive technology and scarce skills globally. Most studies focus on the security of the infrastructure data resides on or the application generating the data. The leaders in research Gartner and Forrester have since noticed a decline in data security research as most entities and security firms are focused on limiting access before a threat actor can reach the physical data store, cloud or on-premise.

The result of the study should indicate the extent financial services take to secure data. What approaches are taken and how are these elements quantified to gauge the Return on Security Investment (ROSI). The rationale for conducting the study "Cybersecurity Perspectives on Protecting Intangible Commodities: A Case Study of Financial Institutions in South Africa" is the increasing importance of cybersecurity in the financial sector in South Africa. With the rapid advancement of technology, financial institutions are exposed to various cyber threats, such as hacking, phishing, malware, and social engineering.

The study seeks to explore the measures that financial institutions in South Africa have implemented to protect their intangible assets from cyber threats. It is essential to understand the extent to which financial institutions in South Africa are vulnerable to cyberattacks and the impact that such attacks can have on their operations, reputation, and financial stability.

Moreover, the study seeks to provide insights into the challenges faced by financial institutions in protecting their intangible assets and the strategies that can be employed

to overcome these challenges. Financial institutions need to be proactive in developing effective cybersecurity strategies that can withstand evolving cyber threats.

The study's findings will contribute to the knowledge and understanding of cybersecurity in the financial sector in South Africa and provide recommendations for improving cybersecurity measures in financial institutions. The study's insights can be valuable to policymakers, financial institutions, and other stakeholders in the financial sector in South Africa and other countries facing similar challenges.

1.7 Delimitations of the study

The study focuses solely on financial institutions in South Africa. It does not cover other countries or regions, and the findings may not be generalisable to other contexts. The study is limited to banks, insurance companies, and other financial institutions operating in South Africa. It does not cover other types of organisations, such as fintech companies, that may also be vulnerable to cyber threats.

The study specifically focuses on the protection of intangible assets, such as intellectual property, customer data, and trade secrets. It does not cover the protection of physical assets or other types of assets. The study focuses on the measures that financial institutions in South Africa have implemented to protect their intangible assets from cyber threats. It does not cover other aspects of cybersecurity, such as cybersecurity governance or the legal and regulatory environment. The study is limited to the current state of cybersecurity in financial institutions in South Africa as of 2023. It does not cover future developments or changes in the cybersecurity landscape.

1.8 Definition of terms

Cybersecurity - Cybersecurity involves comprehending various cyber threats and crafting defence strategies, known as countermeasures, to uphold the confidentiality, integrity, and availability of all digital and information technologies

(Jang-Jaccard & Nepal, 2014). The act of protecting ICT systems and their content has come to be known as cybersecurity (Fischer, 2016).

Cybersecurity perspectives – A theoretical and practical framework of technologies and procedures engineered to safeguard networks, devices, software, and data from a range of cyber threats, harm, or unauthorized entry (Alsharida et al., 2023), (Liang et al., 2023).

Financial Institution – As per the Financial Sector Act 9 of 2017, a financial institution is, (1) A financial Product provider; (2) a financial service provider; (3) a market infrastructure; (4) a holding company of a financial conglomerate; (5) a person licensed or required to be licensed in terms of a financial sector law (Financial Sector Regulation Act 9 of 2017, n.d.). Financial institutions ensure liquidity, guarantee money supply in the economy, provide loans, savings and deposits and ensure payments and settlements are made (Gulyás & Kiss, 2023). Financial Sector has different types of transactions in such areas as real estate, consumer finance, banking and insurance (Asmundson, 2011).

Cyberspace - Cyberspace is the interdependent network of information technology that includes the internet, telecommunications networks, computer systems and internet-connected devices (Page 18, National Cyber Strategy, 2022).

Intangible commodities – Intangible can be defined as identified as a primary factor of production (Tsakanikas et al., 2022). A commodity is defined as a substance or product that can be traded, bought, or sold as per the Cambridge Dictionary. Studies define these commodities as perspectives in various sectors and as such leverage the term assets to account for the value (Moberly, 2014). These include intellectual property, trade secrets, customer data, financial information, and other sensitive information (Demmou et al., 2019), (Grace Smith et al., 2008). Therefore, we can draw that the association between intangible assets and intangible commodities are one and the same.

1.9 Assumptions

As data security is a growing concern across various industries considering the multiple cyber-attacks. The volume of financial service entities is of a mass scale globally and the response rate is estimated to be at 80% confidence. There is a chance that most responses will be provided by South African entities only. Additional assumed factors considered while conducting the research were:

1. Regulatory Compliance: The South African financial sector is subject to regulatory frameworks and standards related to cybersecurity and data protection.
2. Technological Infrastructure: The financial sector in South Africa relies heavily on digital technologies and platforms for operations, making them vulnerable to cyber threats.
3. Human Factor: Human error or insider threats pose significant risks to the security of intangible commodities within the financial sector.
4. Threat Landscape: The threat landscape for cyberattacks targeting the South African financial sector is dynamic and evolving, encompassing various types of threats such as malware, phishing, and ransomware.
5. Resource Constraints: Organisations within the financial sector may have limited resources, including budget, expertise, and technology, to implement robust cybersecurity measures.
6. Collaborative Efforts: Collaboration between public and private sectors, as well as with international partners, is essential for effectively addressing cybersecurity challenges in the South African financial sector.
7. Impact of Global Trends: Global trends such as digital transformation, remote work, and emerging technologies (e.g., blockchain, AI) influence the cybersecurity landscape of the South African financial sector.
8. Consumer Trust: Maintaining consumer trust and confidence is critical for the success and stability of the financial sector, necessitating a focus on

cybersecurity measures to protect intangible commodities, including sensitive customer data.

These assumptions provide a foundational understanding of the context and challenges surrounding cybersecurity in the South African financial sector, which can serve as the basis for further research and analysis in the dissertation. The opinions and influence of legislation, regulators and professionals will be based on the most recent published best practices or acts.

1.10 Chapter Outline

This paper aims to provide a comprehensive overview of cybersecurity perspectives for protecting intangible commodities in financial institutions in South Africa. The paper is structured into six main sections. The first chapter is an Introduction, which provides an overview of the problem statement, the research aims and the objects. The second chapter is the Literature Review, which identifies the key cybersecurity perspectives for protecting intangible commodities in financial institutions as well as the Theoretical Framework, which provides a structured approach to managing information security risks in financial institutions.

The third chapter is the Research Methodology which provides the means and methods used to gather empirical research to support the study of cybersecurity perspectives for protecting intangible commodities in financial institutions. The fourth chapter is the Presentation of Results utilising statistical methods. It aims at explaining the method of cleaning the data collected, performing the analysis and interpreting the results of the tested hypotheses.

The fifth chapter is the Interpretation of the Results where the findings are compared to the literature review concluded in the second chapter and leans into the theoretical frameworks and addresses the research objective outcomes. The final chapter is the Conclusion and Recommendation which contributes to the knowledge and

understanding of cybersecurity in the financial sector in South Africa and provides recommendations for improving cybersecurity measures within financial institutions.

1.11 Conclusion

Cybersecurity is a critical component in the protection of intangible commodities within financial institutions. The findings of this study emphasize the importance of robust cybersecurity measures, continuous monitoring, and the adoption of both local and global frameworks to mitigate cyber threats. By addressing the identified challenges and implementing the proposed recommendations, South African financial institutions can enhance their cybersecurity posture, safeguarding their assets, maintaining regulatory compliance, and preserving their reputation in an increasingly digital world

This study contributes to the understanding of cybersecurity in South Africa's financial sector and provides a foundation for future research and policy development aimed at improving cybersecurity measures in financial institutions.

CHAPTER 2. LITERATURE REVIEW AND THEORETICAL FRAMEWORK

2.1 Introduction

This chapter illustrates the key themes relevant to the study based on academic literature. The literature review focuses on where intangible commodities reside. The importance and challenges faced in cybersecurity by the financial services sector. Supported by the appropriate best practices and frameworks available for use in securing intangible commodities. The conclusion summarises the findings and insights obtained following the literature review.

2.2 Cyberspace

According to the United Kingdom National Cyber Strategy, Cyberspace can be defined as:

"Cyberspace is the interdependent network of information technology that includes the internet, telecommunications networks, computer systems and internet-connected devices." (Page 18, *National Cyber Strategy*, 2022). Cyberspace can be described in terms of three layers, Virtual, Logical and Physical.

The Information and Communication Technology (ICT) sector within South Africa developed in the early 1990s contributed to the cyberspace evolution that has contributed to the increased economic activity seen today (Henwood et al., 2018).



Figure 4. Virtual Layer (*National Cyber Strategy*, 2022)

2.2.1 *Virtual Layer*

This aspect of the online experience (figure 4) is familiar to most individuals. It encompasses the portrayal of people and organisations through a digital identity within a communal virtual environment. These virtual representations might include an email address, user ID, social media account, or an alias, as illustrated in Figure 4. Individuals or organisations may possess multiple online identities, while conversely, multiple entities may share a single, collective identity.



Figure 5. Logical Layer (*National Cyber Strategy*, 2022)

2.2.2 *Logical Layer*

Clark further expands that the logical layer is where decisions are made, in essence, a series of platforms that transmit data (Clark, 2010). Comprising code or data, including operating systems, protocols, applications, and additional software, the logical layer is interdependent with the physical layer. Information traverses wired networks or the electromagnetic spectrum within this layer. Together, the logical and physical layers facilitate communication and action for virtual identities. (Figure 5).

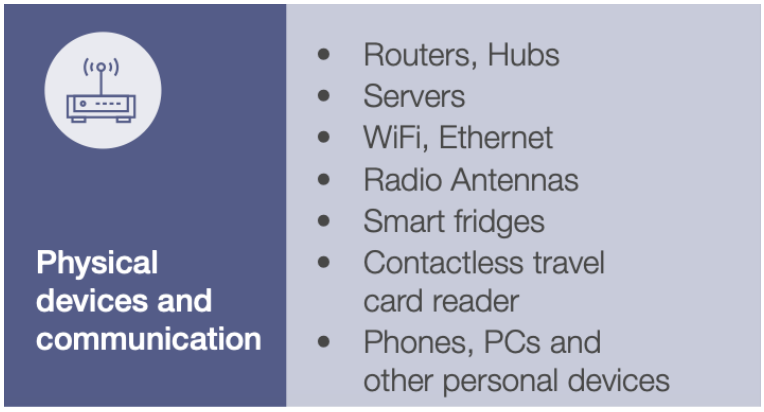


Figure 6. Physical Layer (*National Cyber Strategy*, 2022)

2.2.3 *Physical Layer*

Clark outlines the physical layer of cyberspace as the foundational layer (Clark, 2010). This includes all the hardware on which data is transmitted, from the network hardware, wires and devices that are in residential homes, to large complex telecommunications systems operated by large companies (figure 6).

South Africa's adoption of modern technologies and the internet has created this cyberspace in which individuals and organisations are dependent on for consuming and relaying information. Technology and the internet has become intrinsic and compelling part of our everyday lives (Hunton, 2011).

These three layers work in conjunction to deliver value to the end user and valuable insights for the organisation which flow through the data lifecycle. Stobierski defined the eight steps of the data lifecycle (figure 4) which is an expanded view of the traditional five steps which cover creation, storage, usage, archival and ultimately destruction (Tim Stobierski, 2021).

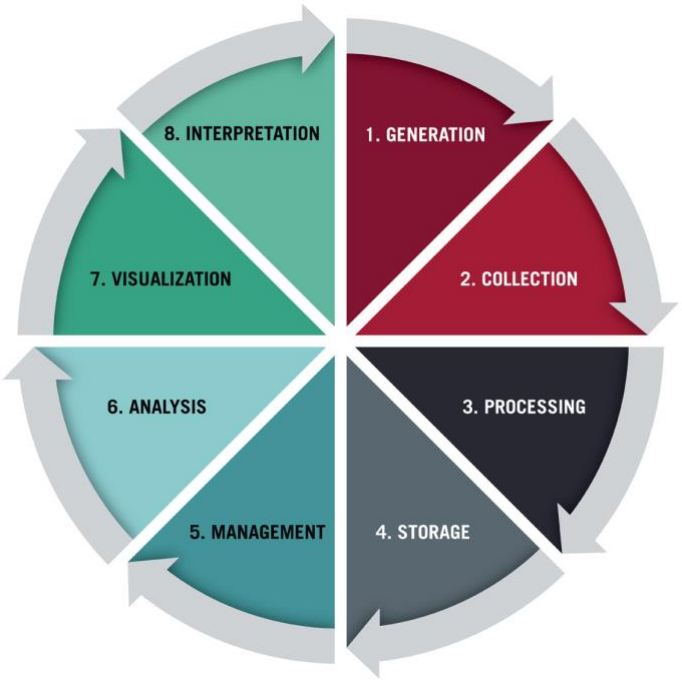


Figure 7. 8 Steps of Data Management Lifecycle (Tim Stobierski, 2021)

2.3 Cybersecurity

Cybersecurity has become an increasingly important topic in recent years due to the growing reliance on technology and the internet in various aspects of daily life. The purpose of this literature review is to explore various research studies and articles on the topic of cybersecurity, including its importance, challenges, and best practices.

2.3.1 *Importance of Cybersecurity*

Cybersecurity is essential to protect individuals and organisations from cyber threats, which can range from identity theft and financial fraud to data breaches and cyber espionage. Cyber-attacks can cause significant financial losses, damage to reputations, and even physical harm. According to the Ponemon Institute's 2020 Cost of a Data Breach Report, the average cost of a data breach is $3.86 million (Ponemon Institute, 2022).

As noted by South African Banking Risk Information Centre (SABRIC), South Africa loses $157 million annually to cyberattacks (Kshetri, 2019). SABRIC currently monitors known threats and aims at educating consumers about the most common scams or fraud activities (figure 8) committed using technology by threat actors. While the list has been growing in the recent year, significant efforts using advanced tactics are involved to ultimately gain access to data.



Figure 8. SABRIC Scam and Fraud Activity (Source: Sabric)

2.3.2 *Challenges of Cybersecurity*

One of the main challenges of cybersecurity is the constantly evolving nature of cyber threats. Hackers and other cybercriminals are constantly developing new tactics and techniques to bypass security measures and gain unauthorised access to systems and data. Although South Africa has made efforts to establish cybersecurity regulations and policies, the implementation and enforcement of these measures face challenges. Keeping pace with rapidly evolving cyber threats requires continuous adaptation and updates to existing frameworks.

Ramezan (2023), explicitly states that while demand for cybersecurity professionals is high, there is a workforce shortage and skills gaps being faced within the field (Ramezan, 2023). Parker and Brown (2019), reinforced this message by analysing 196 unique job advertisements from 5 job portal websites in South Africa where organisations are looking to employ cyber security professionals with a Bachelor's degree in either Computer Science, Information Systems or Engineering as minimum qualification along with industry certifications (Figure 9) and relevant experience (Parker & Brown, 2019). Operational roles require some form of expertise in multiple programming languages, most common languages required are Python, Java and C++.

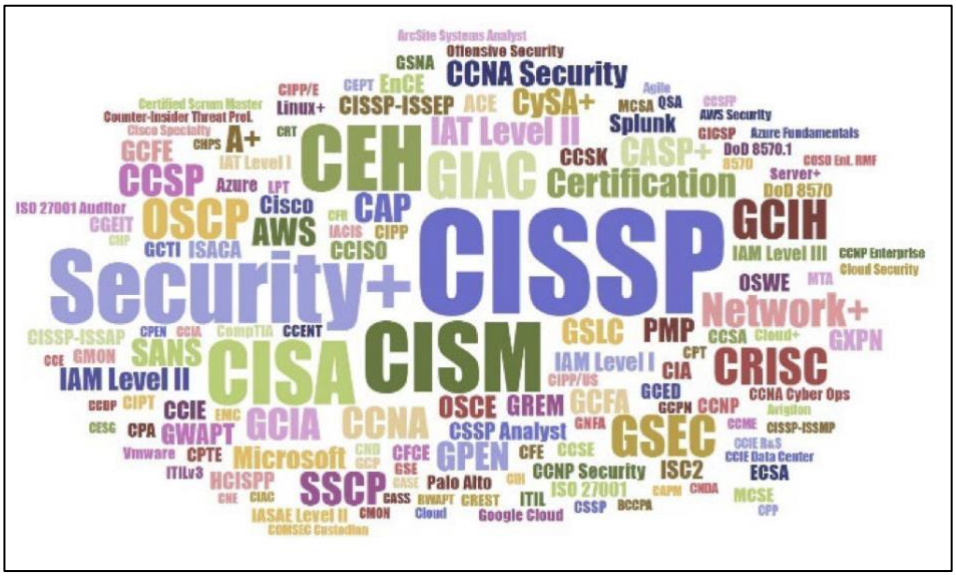


Figure 9. Word Cloud of Industry Certification Listings

There is a general lack of cybersecurity awareness and education among the general population, businesses, and even government entities. Many individuals and organisations are not fully aware of the potential risks and preventive measures needed to safeguard their digital assets. In an article Arthur Goldstruck states, “SA institutions have regularly demonstrated that they are unprepared for the global escalation in cybercrime in recent years”, following the SARB being notified by the FBI about the attack (Maliti, 2022).

While new businesses are starting up it is also noted that small and medium-sized enterprises (SMEs), face resource constraints when it comes to investing in robust cybersecurity infrastructure and tools. This limitation makes them more vulnerable to attacks, as they may lack the necessary funds and expertise to implement comprehensive security measures.

2.3.3 *Best Practices for Cybersecurity*

Aliyu et al., stated there are several best practices that exist that individuals and organisations can follow to improve their cybersecurity (Aliyu et al., 2020). One of the

most important is to use strong passwords and enable two-factor authentication whenever possible. Regularly updating software and using antivirus software can also help prevent cyber-attacks. Organisations should also implement a cybersecurity framework that includes policies, procedures, and training for employees. An illustration of the top known frameworks was conducted to highlight the differences and in most cases the similarities.

ISO 27000 is a series of international standards that provide guidelines and best practices for establishing, implementing, maintaining, and continually improving an information security management system (ISMS). It provides a comprehensive framework for managing the security of an organisation's information assets, including people, processes, and technology. (International Organization for Standardization, 2018, p. 27)

ISO 27001 is a specific standard within the ISO 27000 series. It sets out the requirements for establishing, implementing, maintaining, and continually improving an ISMS. The standard provides a risk-based approach to information security management and focuses on establishing a systematic and structured approach to managing information security risks. (International Organization for Standardization, 2022b, p. 27001)

ISO 27002, also known as ISO/IEC 27002:2013, is a code of practice within the ISO 27000 series. It provides a set of best practices and security controls that organisations can use to implement and manage their information security programs. The standard covers a wide range of security topics, including risk assessment, access control, cryptography, physical security, and incident management. (International Organization for Standardization, 2022a, p. 27002)

ISO 27032 is a standard within the ISO 27000 series that focuses specifically on cybersecurity. It provides guidance for improving the state of cybersecurity, addressing both the technical and organisational aspects. ISO 27032 emphasizes the importance of collaboration and coordination among different stakeholders, including governments,

organisations, and individuals, to enhance cybersecurity resilience. (International Organization for Standardization, 2023, p. 27)

ISO 27000, ISO 27001, ISO 27002, and ISO 27032 are all part of the ISO 27000 family of standards. These focus on information security management systems (ISMS) and provide guidance for organisations to protect their information assets. The ISO 27000 family of standards outlines the terms, definitions, and general concepts related to information security management (ISMS). It provides a risk-based framework for organisations to identify and manage information security risks effectively. The key principle of ISO 27001 is the establishment of an ISMS based on a risk management approach. It emphasizes the importance of continuous improvement, risk assessment, and compliance with legal and regulatory requirements.

The key principle of ISO 27002 is the implementation of a set of information security controls based on risk assessment and organisational needs. It covers various areas of information security, including asset management, access control, cryptography, incident management. The key principle of ISO 27032 is the promotion of cybersecurity as a collective responsibility. It emphasizes the need for organisations to establish strategies, policies, and procedures to manage cybersecurity risks and foster cooperation and collaboration among relevant stakeholders.

The Center for Internet Security (CIS) Controls is a set of best practices that organisations can implement to enhance their cybersecurity defences. The controls provide specific recommendations to address common cyber threats and are organized into three implementation levels: basic, foundational, and organisational. The CIS Controls cover areas such as inventory and control of hardware assets, secure configuration management, and continuous vulnerability assessment and remediation. (*CIS Controls Version 8*, n.d.)

Control Objectives for Information and Related Technologies (COBIT) is a framework developed by the Information Systems Audit and Control Association (ISACA) and the IT

Governance Institute (ITGI). It focuses on IT governance and aligning IT objectives with business goals. COBIT helps organisations establish controls and processes to ensure the effective management of information and technology resources. It covers areas such as risk management, resource management, and incident management. (*COBIT | Control Objectives for Information Technologies*, n.d.)

The MITRE ATT&CK framework is a knowledge base of adversary tactics and techniques used in cyberattacks. It provides a comprehensive catalogue of cyber threat behaviours and serves as a reference for organisations to understand and improve their detection and response capabilities. The framework helps organisations identify gaps in their defences and develop strategies to detect, prevent, and respond to specific attack techniques. (*MITRE ATT&CK®*, n.d.)

NIST stands for the National Institute of Standards and Technology, which is a non-regulatory agency of the United States Department of Commerce. NIST develops and publishes standards, guidelines, and best practices for various areas, including information security and cybersecurity. The most well-known NIST publication related to cybersecurity is the NIST Special Publication 800-53, which provides a comprehensive set of security controls and guidelines for federal information systems. (Force, 2020)

NIST standards are widely adopted not only within the United States government but also by organisations around the world. NIST's cybersecurity framework, specifically the NIST Cybersecurity Framework (CSF), is a risk-based approach that organisations can use to assess and improve their cybersecurity posture. It provides a set of core functions, categories, and subcategories that organisations can customise to meet their specific security needs. It consists of five core functions: Identify, Protect, Detect, Respond, and Recover. (“CSF 2.0 Profiles,” 2024)

Overall, cybersecurity is a critical issue that affects individuals, businesses, and governments. While there are many challenges associated with cybersecurity, there are also several best practices that can be implemented to mitigate the risks of cyber-

attacks. Ongoing research and innovation in the field of cybersecurity are essential to stay ahead of the constantly evolving nature of cyber threats.

2.4 ANALYTICAL FRAMEWORK

2.4.1 *Theoretical Framework*

This paper's theoretical framework is rooted in the General Strain Theory, which was introduced by Robert Merton in 1938. Merton's framework incorporates the concepts of Social Structure and Anomie to explore the relationship between societal norms and individual behaviour (Merton, 1938).

Social Structure, as proposed by Merton, highlights the significant role of society's organisation and institutions in shaping individuals' aspirations and actions. According to Merton, society establishes culturally approved goals and provides accepted means to achieve these goals. These objectives may include material success, wealth, status, and social recognition, while the means to attain them could involve education, hard work, or other legitimate channels.

Merton identified five possible relationships individuals can have with societal norms based on their pursuit of goals and means:

1. Conformity: Individuals who accept both the societal goals and the approved means to achieve them.
2. Innovation: People who accept the goals but resort to unconventional or illegitimate means due to a lack of access to approved channels.
3. Ritualism: Individuals who abandon the pursuit of societal goals but rigidly adhere to the accepted means.
4. Retreatism: Those who reject both the societal goals and the approved means, often leading to a withdrawal from societal norms.

5. Rebellion: Individuals who challenge existing societal goals and means and seek to replace them with their own alternative framework.

Anomie, borrowed by Merton from Emile Durkheim and further developed in his own work, refers to a state of normlessness or breakdown of social norms within a society. Anomie occurs when there is a mismatch between culturally prescribed goals and the available means to achieve them. In such societies, individuals may experience frustration, confusion, and moral ambiguity as they struggle to bridge the gap between their aspirations and the limited opportunities to fulfil them (Merton, 1938; Prof. Elton Mayo, 1934).

Merton argued that anomie could lead to deviant behaviour, as individuals may resort to unconventional or illegitimate means to achieve their goals due to the lack of socially acceptable avenues. For example, if the dominant cultural goal is material wealth, but legitimate means of attaining it (such as through education and employment) are not accessible to everyone, some individuals may turn to criminal activities or other deviant actions as alternatives. To extend on Merton's argument the same concept can be applied to organisations as illustrated in the Selective Organisational Information Privacy and Security Violations Model (SOIPSVM) (Wall et al., 2015).

The concepts of Social Structure and Anomie provide valuable insights into how societal organisation and the availability of opportunities influence individual behaviour, conformity, and deviance. These ideas continue to hold significance in the field of sociology, offering a deeper understanding of human actions within the broader context of social norms and expectations that infringe on information privacy and security violations.

In addition to being rooted in the General Strain Theory (GST), the theoretical framework of this paper can also incorporate the Theory of Reasoned Action (TRA). Developed by Martin Fishbein and Icek Ajzen in the late 1960s, TRA is a social psychology model that aims to predict and understand human behaviour, particularly actions that

individuals consciously control (Sarver, 1983). The theory proposes that people's behavioural intentions are influenced by two key factors: their attitudes toward the behaviour and subjective norms as illustrated in figure 10.

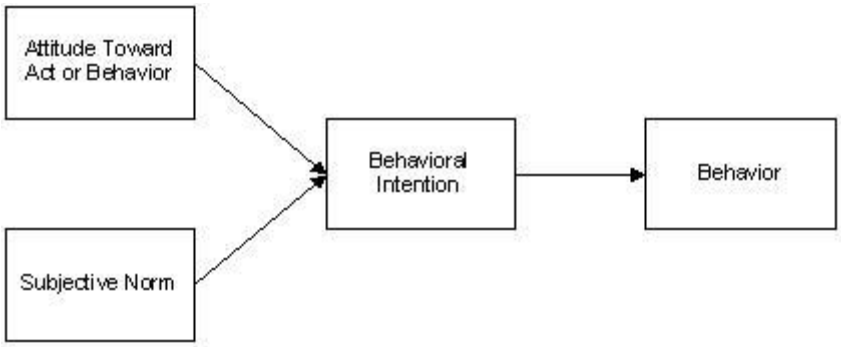


Figure 10. Theory of Reasoned Action (Thomas Sarver Jr., 1983)

Attitudes in the TRA refer to an individual's overall evaluation or perception of a specific behaviour. This includes beliefs about the outcomes or consequences of the behaviour and the person's evaluation of those outcomes as positive or negative. Within the TRA, attitudes focus on behavioural beliefs and the evaluation of the associated outcomes.

Subjective norms, on the other hand, represent the social influences on an individual's behavioural intentions. It involves the perception of societal or peer pressures regarding whether one should or should not engage in a particular behaviour. Subjective norms are shaped by normative beliefs, which are perceptions about what important others think, and the individual's motivation to comply with those beliefs (Madden et al., 1992).

Behavioural intentions are a central aspect of the Theory of Reasoned Action. They indicate an individual's readiness and willingness to engage in a specific behaviour. These intentions are influenced by both attitudes and subjective norms. The stronger the positive attitude toward the behaviour and the stronger the perceived social pressure to engage in it, the more likely the individual is to form a strong behavioural intention to carry out the behaviour (Madden et al., 1992).

According to TRA, behavioural intentions are considered the best predictor of actual behaviour. In many cases, individuals are likely to act in alignment with their intentions (Sarver, 1983). However, other factors, such as external constraints or unexpected circumstances, may also influence whether an individual's intentions translate into actual behaviour.

While the TRA primarily focuses on attitudes and subjective norms, it acknowledges that other factors can indirectly influence behaviour. These additional factors may include individual characteristics (e.g., personality, self-efficacy), situational constraints, and perceived control over the behaviour.

2.4.2 *Conceptual Framework*

The concept of selective organisational information privacy and security violations (SOIPSV) revolves around the idea of organisations intentionally breaching privacy and security measures for specific purposes (Wall et al., 2015). This could involve accessing, sharing, or using sensitive information in ways that are not compliant with ethical, legal, or industry standards.

The Selective Organisational Information Privacy and Security Violations Model (SOIPSVM) as depicted in Figure 11 suggests that organisations that strategically and selectively breach information privacy and security measures for specific purposes will experience short-term benefits such as increased access to competitor information, cost reduction, or improved efficiency. However, in the long run, such organisations are more likely to face severe negative consequences, including legal penalties, reputational damage, loss of customer trust, and decreased employee morale, leading to overall detrimental effects on the organisation's performance and sustainability (Wall et al., 2015).

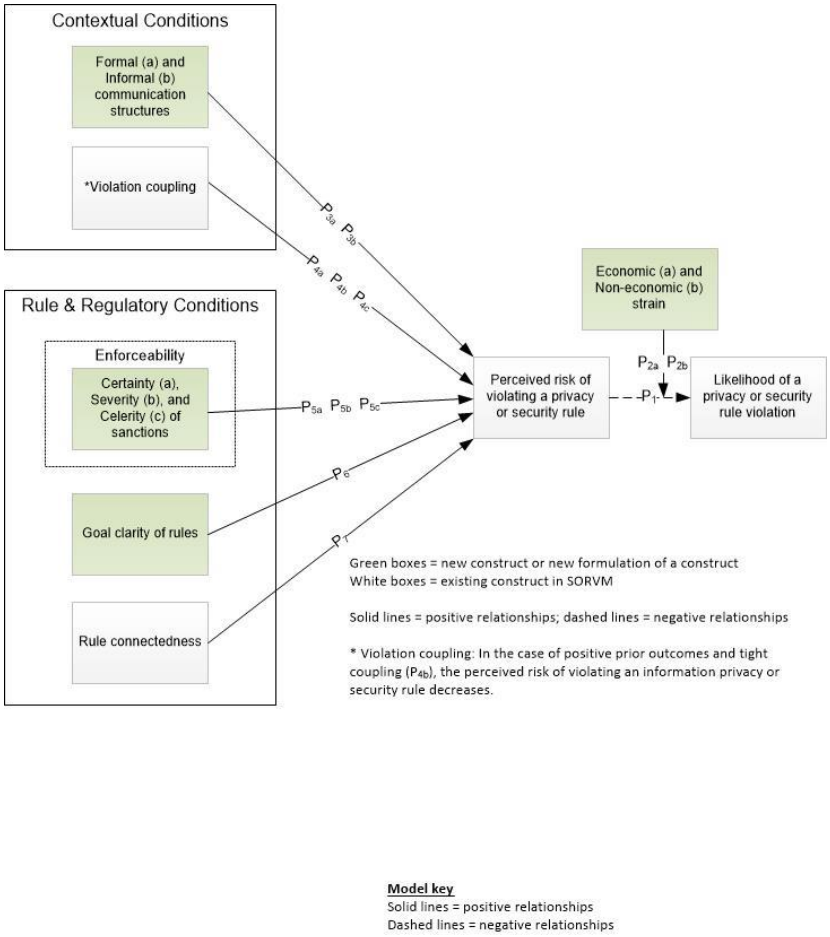


Figure 11. Overview of the selective organisational information privacy and security violations model (SOIPSVM), (Source: (Wall et al., 2015))

Organisations implement information practice in three ways as outlined by Wall et al, (2015).

1. Government Regulation
2. Self-regulation
3. Technological solutions

The interplay between contextual conditions, rule characteristics, perceptions of risk, and focus of attention forms a complex web of influences on organisational decision-making and behaviour related to rule compliance. Understanding and managing these factors effectively can be critical for promoting a culture of ethical conduct and minimising the occurrence of rule violations within the organisation.

2.5 Hypothesis

Considering the Selective Organisational Information Privacy and Security Violations Model (SOIPSVM) to support the research aim to provide a comprehensive overview of cybersecurity perspectives for protecting intangible commodities in financial institutions in South Africa. The following hypothesis can be drawn that remains to be tested.

H1: The perceived risk of violating a privacy or cybersecurity rule negatively affects the likelihood of a privacy or security rule violation aimed at safeguarding intangible commodities.

This hypothesis suggests that if individuals or organisations perceive a high risk associated with violating privacy or cybersecurity rules, they will be less likely to engage in actions that could compromise the security of intangible assets, such as sensitive information, digital assets, or intellectual property (Rachida Parks et al., 2016).

H2: Both formal and informal communication structures that promote regulatory compliance will heighten the perception of risk regarding rule violation for individuals and organisations.

This hypothesis suggests that effective communication structures, both formal (such as official policies) and informal (such as workplace culture), that emphasize compliance with privacy and cybersecurity regulations can lead to an increased perception of risk related to rule violations (Albshaier et al., 2024; Shaikh & Siponen, 2023). In other words, when individuals and organisations are consistently reminded and encouraged to comply with regulations, they may be more cautious and fearful of the consequences of non-compliance.

H3: Instances of violations linked to negative outcomes will increase the perception of risk associated with rule violation for individuals and organisations.

This hypothesis suggests that when individuals or organisations witness or experience actual violations of privacy or cybersecurity rules that lead to negative consequences, it will heighten their perception of risk associated with rule violations (Rachida Parks et al., 2016). Observing the negative outcomes of others' non-compliance may serve as a deterrent, making them more cautious about breaking the rules themselves.

H4: The enforceability of regulations will positively impact the perception of risk of rule violation for individuals and organisations.

This hypothesis suggests that when privacy and cybersecurity regulations are effectively enforced, individuals and organisations are more likely to perceive a higher risk associated with rule violations (Shaikh & Siponen, 2023; W. Alec Cram et al., 2017). If there is a higher chance of facing consequences for non-compliance due to robust enforcement, it may dissuade them from engaging in risky behaviour.

H5: The clarity of goals in rules and regulations will positively influence the perception of risk of violating those rules for individuals and organisations.

This hypothesis proposes that if privacy and cybersecurity rules and regulations are clear and unambiguous, individuals and organisations will perceive a higher risk associated with violating those rules(Jeffrey D. Wall et al., 2016). When the rules are well-defined,

there is less room for interpretation, making it easier for individuals and organisations to understand the potential consequences of non-compliance.

H6: Connectedness (referring to network connections or relationships) will positively influence the perception of risk of violating rules for individuals and organisations.

This hypothesis suggests that individuals and organisations with more extensive network connections or relationships (within a professional context) may have a higher perception of risk related to rule violations (Jeffrey D. Wall et al., 2016). It's possible that being connected to a broader network exposes them to more information about the potential consequences of non-compliance or that they receive peer pressure to adhere to the rules.

H7: A positive attitude towards rule-abiding behaviour will positively influence the perception of risk of violating rules for individuals and organisations.

This hypothesis proposes that individuals and organisations with a positive attitude towards following rules and regulations will perceive a higher risk associated with violating them (Alyami et al., 2023). A strong internal commitment to rule compliance can lead to increased vigilance and caution when considering potential rule violations.

H8: Subjective norms will positively influence the perception of risk of violating rules for individuals.

This hypothesis suggests that individuals' perceptions of societal or group norms related to privacy and cybersecurity rule compliance will impact their perception of risk associated with violating these rules (Rachida Parks et al., 2016; Sangmi Chai, 2009). If individuals believe that their peers or society at large values compliance, they may feel a higher perceived risk when considering rule violations.

2.6 Conclusion of Literature Review

This chapter explored key themes relevant to the study of cybersecurity and the protection of intangible commodities within financial institutions in South Africa. The literature review focused on the importance and challenges faced in cybersecurity, supported by best practices and frameworks available for securing intangible commodities.

Cyberspace, defined as the interdependent network of information technology, consists of three layers: the Virtual, Logical, and Physical layers. These layers work together to deliver value to end-users and organisations, forming the foundation of modern technological advancements.

Cybersecurity emerged as a critical aspect of protecting intangible commodities, given the growing reliance on technology and the internet. The importance of cybersecurity lies in safeguarding individuals and organisations from various cyber threats, which can lead to significant financial losses, reputational damage, and even physical harm.

However, challenges exist in this domain, including the constantly evolving nature of cyber threats, workforce shortages and skills gaps in the cybersecurity field, a lack of cybersecurity awareness, and resource constraints for small and medium-sized enterprises (SMEs).

To address these challenges and improve cybersecurity, various best practices and frameworks are available. These include using strong passwords and two-factor authentication, regularly updating software, employing intrusion detection systems, and implementing cybersecurity frameworks such as ISO/IEC 27001 and NIST Cybersecurity Framework.

The analytical framework of the study focused on identifying intangible commodities and cybersecurity threats, evaluating current cybersecurity measures, identifying gaps, and developing a comprehensive cybersecurity strategy. Following this framework,

financial institutions in South Africa can better protect their intangible commodities from cyber threats.

The theoretical framework of the study integrated the General Strain Theory (GST) and the Theory of Reasoned Action (TRA). GST explored how societal norms and opportunities influence individual behaviour, while TRA examined how attitudes and subjective norms shape behavioural intentions.

The conclusion suggests that the Selective Organisational Information Privacy and Security Violations Model (SOIPSVM) may be relevant to understanding cybersecurity perspectives in financial institutions. Hypotheses have been proposed to test the relationship between cybersecurity practices and the protection of intangible commodities within financial organisations.

In conclusion, this literature review provides valuable insights into the importance and challenges of cybersecurity, as well as best practices and frameworks that financial institutions in South Africa can adopt to protect their intangible assets effectively. By embracing these practices, organisations can create a more secure and resilient cybersecurity environment to safeguard their information and maintain the trust of their stakeholders. Further research and empirical studies will be essential to validate the proposed hypotheses and deepen our understanding of cybersecurity in the financial services sector and extending on the current research of Selective Organisational Information Privacy and Security Violations Model (SOIPSVM).

CHAPTER 3. RESEARCH METHODOLOGY

3.1 Research Approach

This is an empirical study that tests the hypothesis as derived from the Selective Organisational Rule Violations Model (SOVRM). A quantitative research approach is used to obtain a view of industry specialists in South Africa and more specifically the financial services sector.

The study follows a quantitative approach to understanding the depth and magnitude of the problem statement in relation to Cybersecurity perspectives on protecting intangible commodities. Quantitative research provides broader trends and generalisations while qualitative provides a more granular view (John Ward Creswell & John David Creswell, 2022).

A quantitative survey approach has been used to gather relevant information that supports the investigation in a cost-effective manner. The survey has been distributed amongst the financial service industry and to C suite, middle and junior management while maintaining honest and reliable data.

3.2 Research Paradigm

The research paradigm would incorporate elements from various theoretical perspectives to address the complex interplay of factors involved (Kivunja & Kuyini, 2017). The institutional Theory (INT) perspective examines how organisations conform to and diverge from institutional norms and pressures (Shrum, 2001). Resource Dependence Theory (RDT) paradigm focuses on how organisations manage their dependencies on external resources, including regulatory legitimacy (Hillman et al., 2009) . Given the diverse cultural context of South Africa, Cultural Dimensions will be used to understand how cultural values, beliefs, and societal norms shape organisations'

attitudes towards rule violation and the protection of intangible commodities (Chatman & O'Reilly, 2016).

The ethical and Moral Perspectives paradigm emphasizes the ethical dimensions of organisational behaviour and decision-making (Seals, 2013). Which explores how ethical considerations influence organisations' propensity to engage in selective rule violation or adhere to regulatory standards. Finally incorporate insights from legal and regulatory theories to understand the impact of regulatory environments on organisations' behaviour and compliance practices (Bora, 2017).

By integrating elements from these theoretical perspectives, the research paradigm for a Selective Organisational Rule Violation Model in South African financial institutions could provide a comprehensive understanding of the complex dynamics surrounding the protection of intangible commodities and the factors influencing organisations' decisions to adhere to or violate rules in this context.

3.3 Research Design

The research design refers to the overall plan or structure of a research paper (John Ward Creswell & John David Creswell, 2022). This paper aims to provide a comprehensive overview of cybersecurity perspectives for protecting intangible commodities in financial institutions in South Africa. A quantitative research method was selected as the preferred method which will be used to measure the correlations between variables and findings.

The survey method has been chosen as a suitable tool to extract information for the research problem. The online means for distribution allows the respondents to complete the survey remotely at their convenience. The data collected test the relationship between cybersecurity practices and the protection of intangible commodities within financial organisations. Supplementary data from regulators and statistical bodies was considered to support the research if necessary. This

supplementary information is audited and could provide a point of departure that underpins the research questions posed that influence the effectiveness of current cybersecurity measures in South Africa financial institutions.

3.4 Data Collection Method

The data collection methods utilised the Qualtrics online platform, which hosted the self-administered survey. All data collected is considered primary data, demographics and geographics are a functional requirement. Roopa and Rani (2012), define a questionnaire as a series of questions asked to individuals to obtain statistically useful information about a given topic. They further state how questionnaires are the backbone of surveys which are a valuable method of collecting a wide range of information from a large number of individuals, often referred to as respondents (Roopa & Rani, 2012). The study distributes, collects and summarises the data utilising the Qualtrics platform.

Supplementary information sources from statistical institutions specialising in South African data will also be used be it free or paid and the relevance to the study and be considered as secondary data.

3.5 Population and Sample

3.5.1 *Population*

The population of the study is targeted at technology professionals or leaders that have influence in relation cybersecurity within the financial services industry. The financial services industry is highly regulated, and most organisations have pivoted to take on or follow a digital transformative strategy ranging from small to large projects. These strategies are influenced by the decisions and directions of the participant categories outlined:

- C-level executives
- Directors
- Associate directors
- Enterprise Architects
- Middle management
- Junior Management

3.5.2 *Sample and sampling method*

No database exists for all financial institutions in South Africa and therefore a manual database was created from several sources and concatenated to form a master list (Table 2) as base for the population. Based on the specific business operating environment mixed industries will be included in the sample. The sampling method used was consecutive sampling (Ndiga et al., 2014) across the financial services industry.

Institution	Total
Bank	19
Composite	8
Life Insurer	83
Non-Life Insurer	92
Credit Rating Agency	6
Securities	45
Securities and Hedge Funds	1
Property	3
Hedge Funds	2
Benefit administrator & Investment manager	15
Benefit administrator (Professional)	132
Benefit administrator (Employer)	28
Total	434

Table 2. Manual Database of Financial Institutions

Inclusion Criteria	Exclusion Criteria
• C-level executives • Directors • Associate directors • Enterprise Architects • Middle management • Junior Management	• Contractors (Professional Services) • Interns/ Graduates

Table 3. Target Criteria

Utilising the consecutive sampling method, data is being solicited is regarded as primary and objective from the respondent's viewpoint. 400 respondents (Table 4) that meet the criteria of working in financial services and hold the positions outlined (Table 3) are projected to provide information to support and provide further knowledge in relation to the hypothesis for cybersecurity perspectives for protecting intangible commodities in financial institutions in South Africa.

Position	Bank	Composite	Life Insurer	Non-Life Insurer	Credit Rating Agency	Securities	Securities and Hedge Funds	Property	Hedge Funds	Benefit administrator & Investment manager	Benefit administrator (Professional)	Benefit administrator (Employer)	Total
C-level executives	4	1	2	2	1	2	1	1	1	2	2	2	21
Directors	10	2	4	4	1	4	1	1	1	4	4	4	40
Associate directors	16	5	10	10	1	10	1	1	1	10	10	10	85
Enterprise Architects	15	5	10	10	1	10	1	1	1	10	10	10	84
Middle management	16	5	10	10	1	10	1	1	1	10	10	10	85
Junior Management	16	5	10	10	1	10	1	1	1	10	10	10	85
Total	77	23	46	46	6	46	6	6	6	46	46	46	400

Table 4. Target Sample Size

3.6 Research Instrument

An online survey questionnaire is to be used to collect data for the study using the Likert 5-point scale the Qualtrics online platform. The online survey is divided into three sections to allow the identification of the response rate, monitor the collection of data in relation to the research objectives and hypothesis. The questions were structured as follows:

- The demographics section focused on obtaining information about the business and services offered and strategic considerations.
- Questions developed around testing the hypothesis using the Likert 5-point scale associated with Likelihood, Level of Concern, Agreement, Frequency and Importance (Table 5).

Scale	Likelihood	Level of Concern	Agreement	Frequency	Importance
1	Very Unlikely	Very Unconcerned	Strongly Disagree	Never	Very Unimportant
2	Unlikely	Unconcerned	Disagree	Rarely	Unimportant
3	Neutral	Neutral	Neutral	Sometimes	Neutral
4	Likely	Concerned	Agree	Often	Important
5	Very Likely	Very Concerned	Strongly Agree	Always	Very Important

Table 5. Likert 5-point scale used

3.7 Data Analysis and Interpretation

Data analysis is the process of inspecting, cleansing, transforming, and modelling data to extract useful information, draw conclusions, and support decision-making. It involves applying various techniques and methods to understand patterns, relationships, and trends within a dataset. Data interpretation is the process of analysing and making sense of the results obtained from data analysis. It involves extracting meaningful insights, drawing conclusions, and deriving actionable implications from the analysed data (Flick, 2013).

The responses received will be analysed using IBM SPSS. A descriptive analysis will be done to determine key themes or similarities among the respondents. Inferential statistics will follow to test the hypothesis by assessing the relationships between variables on the sample. Multiple regression analyses will be used with the use of comparison tests to draw insights into the defined hypothesis.

Inferential statistics will be used to employ measurements obtained from the sample of participants to contrast the sample groups and draw broader conclusions about the overall population of participants. Structural Equation Modelling (SEM) has also been chosen due to its ability to concurrently conduct multiple regression analyses while accounting for measurement errors during the estimation procedure (Nunkoo & Ramkissoon, 2011).

The validity of responses will be assessed, and an interpretation of the findings conducted.

3.8 Reliability and Validity

The reliability and validity of the study are critical aspects that ensure the trustworthiness and credibility of its findings.

3.8.1 *Reliability*

The study demonstrates reliability through internal consistency by utilising established scales and methods for data collection. Likert scales are used to measure responses consistently across survey participants, enhancing the reliability of the data.

Although not explicitly mentioned, the study could potentially establish test-retest reliability by conducting a pilot study or re-administering the survey to a subset of participants after a period to assess the stability of responses over time. In cases where multiple raters are involved in data collection or analysis, inter-rater reliability ensures consistency in their judgments or evaluations. However, since the study primarily relies on self-administered surveys, inter-rater reliability may not be applicable.

3.8.2 *Validity*

The study demonstrates content validity by aligning research questions and objectives with established theories and literature in cybersecurity and financial services. Additionally, the use of Likert scales and structured survey questions enhances content validity by ensuring that items measure the intended constructs.

Construct validity is established by theoretically grounding the study in relevant frameworks and models, such as the Selective Organisational Rule Violations Model (SOVRM) and theoretical perspectives like Institutional Theory, Resource Dependence Theory, Cultural Dimensions, Ethical and Moral Perspectives, and legal and regulatory theories. This alignment ensures that the study measures the intended constructs related to cybersecurity perspectives and practices.

Criterion validity refers to the degree to which the study's measures correlate with external criteria or gold standards. While the study may not explicitly address criterion validity, it can indirectly demonstrate this by comparing its findings with established benchmarks, industry standards, or regulatory requirements. Face validity is evident in the study through the clear and logical presentation of research questions, objectives,

and methodologies. The study's comprehensiveness and alignment with the research problem contribute to its face validity.

Overall, the study exhibits strong reliability through consistent data collection methods and potential test-retest reliability measures. Additionally, it demonstrates validity by aligning with established theories, using structured survey instruments, and ensuring logical coherence between research questions and objectives.

3.9 Limitations of the study

While cybersecurity is a growing trend amongst various industries within South Africa, we can assume the secret and confidentiality to disclose information might limit the studies efficacy. The organisation in financial service industry is highly regulated and clearance to participate and complete the survey will be done with anonymity.

3.10 Ethical Considerations

This research project adheres strictly to all the ethical guidelines set forth by Wits University. All participants have been fully informed about the purpose of the research, ensuring transparency and understanding of their involvement. They have been given the freedom to decide whether or not to participate and are assured that their data will be used solely for analysis purposes. Throughout the entire research process, the rights and well-being of all participants, including respondents, researchers, and anyone else involved, will be diligently safeguarded. Participants had the right to withdraw from the study at any point they desired.

Data collection was carried out through a secure online survey tool (Qualtrics). The collected data is stored in an accredited database with an access-controlled account that strictly follows security best practices.

This research is conducted without any form of discrimination based on age, gender, or race. Additionally, the research poses no threat to the physical environment and had no adverse impact on it. This research has been conducted with the full approval and oversight of the board of Wits University.

CHAPTER 4. PRESENTATION OF RESULTS

4.1 Introduction

This study aimed to gather input from technology professionals or influential leaders in cybersecurity with the financial sector of South Africa. The study obtained a view across a diverse range of characteristics, including gender, age, years of experience with the industry and Job title. A total of 600 questionnaires were disseminated, with 519 responses received. Data cleansing occurred on the 519 responses received which resulted in 156 deemed as inconsistent data, the survey results demonstrated the participant's response was abandoned and hence incomplete, these records were then deleted and disregarded. It was finalised that 363 responses were deemed usable and formed the basis of this study.

4.2 Demographic Analysis

Demographic statistics were used to obtain a description of the sample. Table 6 shows the demographic characteristics of the participants (n = 363). There were more males (69.70%) than females (30.30%). The majority were in the age group of 35 – 44 (51.52%) followed by 45 – 54 (30.30%). This represented the working group of 35 – 54 forming the bulk of all responses which account for 81.82%. The response rate from Banks (78.79%) surpassed all other industries with a good response from credit rating agencies (12.67%) with the majority of the responses received from participants with greater than 10 years of experience (90.91%).

Demographic Characteristics (N = 363) Variable	*N*	*%*
Gender		
Female	*110*	*30.30%*
Male	*253*	*69.70%*
Age Group		
25 - 34 Years Old	*33*	*9.09%*
35 - 44 Years Old	*187*	*51.52%*
45 - 54 Years old	*110*	*30.30%*
55 - 64 Years old	*33*	*9.09%*
Industry		
Bank	*286*	*78.79%*
Credit Rating Agency	*46*	*12.67%*
Non-Life Insurer	*27*	*7.44%*
Securities	*4*	*1.10%*
Years of Experience		
4 - 6 Years	*11*	*3.03%*
7 - 10 Years	*22*	*6.06%*
More than 10 Years	*330*	*90.91%*

Note. N = 363; % = 100

Table 6. Demographic Analysis

4.3 Descriptive Analysis

4.3.1 *Reliability and Validity Analysis*

A reliability assessment was conducted utilising the Cronbach's Alpha coefficient. Cronbach Alpha values vary between zero and one, with values closer to 1.00 indicating greater consistency and reliability of the constructs (Cronbach, 1949). Cronbach also indicate ideally, reliability should fall within a Cronbach Alpha range of 0.7 or higher. The

analysis confirmed the reliability of the constructs, with all statistics surpassing 0.7. Additionally, the lowest and highest values were 0.745 and 0.856, respectively. Refer to Table 7 for detailed results. The Convergent Validity aims to ensure the Average variance extracted is greater than 0.5 (Cohen, 1988), the lowest and highest values were 0.505 and 0.874.

While the 'Attitude towards Behaviour' and 'Enforceability' construct exhibits acceptable reliability based on Cronbach's alpha and composite reliability, the average variance extracted suggests that the items may not fully capture the construct's variability. The remaining construct show good reliability and internal consistency, supported by both Cronbach's alpha and composite reliability. Additionally, the high average variance extracted indicates that the items effectively capture a significant portion of the construct's variance.

	Cronbach's alpha	**Composite reliability (rho_a)**	**Composite reliability (rho_c)**	**Average variance extracted (AVE)**
Attitude towards Behaviour	0.793	0.811	0.856	0.544
Communication Structures	0.752	0.817	0.887	0.797
Enforceability	0.758	0.789	0.834	0.505
Goal Clarity of Rules	0.856	0.857	0.933	0.874
Rule Connectedness	0.745	0.770	0.886	0.795
Subjective Norms	0.821	0.818	0.875	0.586
Violation Coupling	0.821	0.858	0.869	0.531

Table 7. Construct Reliability and Validity Overview

The variables were analysed in table 8 utilising descriptive statistics. Mean and Standard Deviation provide insights into the central tendency and variability of the data. Excess Kurtosis indicates the presence and degree of outliers compared to a normal distribution. Positive values indicate heavier tails, while negative values indicate lighter tails. Skewness describes the symmetry of the distribution. Positive skewness means a

longer tail on the right, negative skewness means a longer tail on the left, and zero skewness implies perfect symmetry.

Name	N	Mean	Standard deviation	Excess kurtosis	Skewness
H1.1	363	4.879	0.326	3.452	-2.331
H1.2	363	3.152	1.520	-1.475	-0.154
H1.3	363	4.727	0.445	-0.955	-1.025
H1.4	363	4.576	0.605	0.221	-1.120
H1.5	363	4.333	0.682	-0.780	-0.534
H2.1	363	4.667	0.586	1.432	-1.579
H2.2	363	3.939	0.886	-0.668	-0.407
H2.3	363	4.242	0.605	-0.532	-0.171
H2.4	363	4.030	0.797	-0.459	-0.415
H2.5	363	3.970	0.758	-0.212	-0.368
H3.1	363	2.455	0.820	-0.454	0.312
H3.2	363	4.273	0.708	-0.933	-0.446
H3.3	363	4.303	0.758	0.735	-0.989
H3.4	363	4.333	0.636	-0.683	-0.421
H3.5	363	4.455	0.742	1.773	-1.406
H4.1	363	3.970	0.870	-0.473	-0.496
H4.2	363	4.182	0.672	-0.812	-0.234
H4.3	363	4.000	0.888	-0.550	-0.522
H4.4	363	4.182	0.796	-0.097	-0.700
H4.5	363	4.152	0.744	-1.162	-0.252
H5.1	363	3.939	0.776	-0.443	-0.285
H5.2	363	4.030	0.577	0.017	0.000
H5.3	363	4.000	1.044	-0.547	-0.801
H5.4	363	3.667	0.765	0.058	-0.573
H5.5	363	3.212	1.066	-0.524	-0.130
H6.1	363	4.182	0.796	-1.350	-0.338
H6.2	363	3.848	0.892	-0.870	-0.213
H6.3	363	3.879	1.122	-0.298	-0.795
H6.4	363	3.909	0.965	1.027	-1.036
H6.5	363	3.939	0.919	-0.452	-0.585
H7.1	363	4.727	0.509	2.014	-1.695
H7.2	363	4.424	0.653	-0.548	-0.702
H7.3	363	4.394	0.694	-0.678	-0.710
H7.4	363	4.394	0.736	1.476	-1.232
H7.5	363	4.182	0.716	-1.024	-0.284
H8.1	363	3.333	1.035	-0.637	-0.043
H8.2	363	3.364	1.010	-0.577	-0.245
H8.3	363	3.848	0.744	0.520	-0.636
H8.4	363	3.515	0.925	0.213	-0.736
H8.5	363	3.273	0.993	-0.651	-0.196

Table 8. Descriptive statistics

Table 8 depicts the descriptive analysis which indicate H1.1 to H7.5 variables have means ranging from approximately 2.45 to 4.88 and standard deviations ranging from around 0.33 to 1.52. They exhibit various degrees of excess kurtosis and skewness. H8.1 to H8.5 variables have means ranging from approximately 3.27 to 3.85 and standard deviations ranging from around 0.74 to 1.04. Further analysis is grouped by construct below.

4.3.2 *Violation Coupling*

These variables demonstrate different distributions in terms of central tendency, variability, and shape. H1.1 stands out with the highest excess kurtosis (3.452) and skewness (-2.331), indicating a distribution with heavy left tails and potentially more extreme values. H1.2 and H1.5 have lighter tails and less pronounced skewness. H1.3 and H1.4 share similar characteristics in terms of mean and standard deviation but differ in kurtosis and skewness, suggesting variations in their distributions.

4.3.3 *Communication Structures*

Variables H2.1, H2.2, and H2.3 have higher means and moderate standard deviations, indicating less variability around the mean. H2.1 has heavier tails and a pronounced left skew, while H2.2 and H2.3 have lighter tails and nearly symmetrical distributions. H2.4 and H2.5 have lower means and moderate standard deviations, with lighter tails and slight left skewness.

4.3.4 *Rules Connectedness*

Variables H3.1 to H3.5 represent a set with varying means and distributions. H3.5 stands out with the highest mean (4.455) and pronounced left skewness (-1.406). Variables H6.1 to H6.5 exhibit moderate variability around the mean. H6.4 stands out with heavier tails than the rest, while the others have lighter tails. Additionally, all variables show left-skewed distributions, albeit to varying degrees.

4.3.5 *Enforceability*

Variables H4.1 to H4.5 have similar means but varying levels of variability around the mean. They exhibit slight to moderate left skewness, with varying degrees of excess kurtosis indicating lighter tails compared to a normal distribution.

4.3.6 *Goal Clarity of Rules*

Variables H5.1, H5.4, and H5.5 exhibit moderate variability around their means, while H5.2 shows less variability. H5.3 has the highest variability. The excess kurtosis and skewness vary across the variables, indicating differences in the shape and tail behaviour of their distributions.

4.3.7 *Attitude towards Behaviour*

All variables (H7.1 to H7.5) have means around 4.4, indicating that they are centered around a similar value. They also exhibit left-skewed distributions, with varying degrees of excess kurtosis and skewness. H7.1 has the highest excess kurtosis (2.014), indicating the heaviest tails, while H7.5 has the lowest excess kurtosis (-1.024), indicating the lightest tails among the variables.

4.3.8 *Subjective Norms*

Variables H8.1, H8.2, and H8.5 have relatively symmetrical distributions with lighter tails, while H8.3 and H8.4 have left-skewed distributions with heavier tails, especially H8.4 (-0.736).

4.4 Factor Analysis

Table 8 provides insights from the respondents concerning the constructs and analysis of the variables conducted subsequently (Kock, 2019). The responses to the constructs

were favourable with the majority above the neutral and on the higher end of the 5-point Likert scale.

Construct	Mean	Standard deviation	Excess kurtosis	Skewness	Cramér-von Mises test statistic
Communication Structures 1	4.030	0.797	-0,459	-0,415	4.296
Communication Structures 2	3.970	0.758	-0,212	-0,368	5.107
Enforceability 1	3.970	0.870	-0,473	-0,496	3.797
Enforceability 2	4.182	0.672	-0,812	-0,234	5.845
Enforceability 3	4.000	0.888	-0,550	-0,522	3.671
Enforceability 4	4.182	0.796	-0,097	-0,700	4.670
Enforceability 5	4.152	0.744	-1,162	-0,252	4.613
Goal Clarity of Rules 1	3.939	0.776	-0,443	-0,285	4.596
Goal Clarity of Rules 2	4.030	0.577	0,017	0,000	9.472
Attitude towards Behaviour 1	4.727	0.509	2,014	-1,695	15.605
Attitude towards Behaviour 2	4.424	0.653	-0,548	-0,702	7.050
Attitude towards Behaviour 3	4.394	0.694	-0,678	-0,710	6.577
Attitude towards Behaviour 4	4.394	0.736	1,476	-1,232	6.541
Attitude towards Behaviour 5	4.182	0.716	-1,024	-0,284	5.009
Rule Connectedness 1	4.182	0.796	-1,350	-0,338	4.659
Rule Connectedness 2	3.848	0.892	-0,870	-0,213	3.316
Subjective Norms 1	3.333	1.035	-0,637	-0,043	2.549

Subjective Norms 2	3.364	1.010	-0,577	-0,245	2.808
Subjective Norms 3	3.848	0.744	0,520	-0,636	7.367
Subjective Norms 4	3.515	0.925	0,213	-0,736	5.180
Subjective Norms 5	3.273	0.993	-0,651	-0,196	2.931
Violation Coupling 1	4.727	0.445	-0,955	-1,025	15.275
Violation Coupling 2	4.333	0.682	-0,780	-0,534	5.987
Violation Coupling 3	4.273	0.708	-0,933	-0,446	5.393
Violation Coupling 4	4.303	0.758	0,735	-0,989	5.617
Violation Coupling 5	4.333	0.636	-0,683	-0,421	6.651
Violation Coupling 6	4.455	0.742	1,773	-1,406	7.622

Table 9. Indicator Data

4.4.1 *Communication Structures*

The means close to 4 indicates a relatively positive perception of the construct. Standard deviation suggests variability in responses and is seen as moderate. The nearly normal distribution of data is indicated by the acceptable range for skewness and kurtosis values. The Cramér-von Mises test statistic indicates good model fit.

4.4.2 *Enforceability*

Enforceability means ranging from approximately 3.97 to 4.18 indicates a generally positive perception. Standard deviations vary which suggest some inconsistency in responses. Skewness and kurtosis values are generally within acceptable limits, indicating nearly normal distributions. Cramér-von Mises test statistic indicates a reasonable model fit.

4.4.3 *Goal Clarity of Rules*

Means for Goal Clarity of Rules items range from about 3.94 to 4.03, indicating a positive perception overall. Standard deviations suggest moderate variability while Skewness and kurtosis values indicate nearly normal distributions. Cramér-von Mises test statistic suggests a good model fit.

4.4.4 *Attitude towards Behaviour*

Attitude towards Behaviour construct demonstrate means ranging from approximately 4.18 to 4.73, indicating generally positive attitudes. Standard deviations vary but generally indicate some variability. As some responses exhibit high skewness and kurtosis, suggesting potential non-normality in their distributions. The Cramér-von Mises test statistic indicates a reasonable model fit.

4.4.5 *Rule Connectedness*

Rule Connectedness means close to 4, suggest a moderately positive perception with standard deviations indicating moderate variability. Skewness and kurtosis values suggest nearly normal distributions and the Cramér-von Mises test statistic suggests a good model fit.

4.4.6 *Subjective Norms*

Means for Subjective Norms items range from approximately 3.27 to 3.85, indicating varied perceptions. Standard deviations vary, indicating variability in responses with Skewness and kurtosis values suggest nearly normal distributions for most responses. The Cramér-von Mises test statistic suggests a reasonable model fit.

4.4.7 *Violation Coupling*

Violation Coupling construct exhibit means ranging from about 4.27 to 4.73, indicating generally negative perceptions. The standard deviations suggest moderate variability and some items which exhibit high skewness and kurtosis, indicating potential non-normality. The Cramér-von Mises test statistic suggests a reasonable model fit.

4.5 Hypothesis Testing

The research hypothesis tested whether the Selective Organisational Information Privacy and Security Violations Model (SOIPSVM) was supported by the empirical data, and is presented below:

H1. The perceived risk of violating a privacy or cybersecurity rule negatively affects the likelihood of a privacy or security rule violation aimed at safeguarding intangible commodities.

H2. Both formal and informal communication structures that promote regulatory compliance will heighten the perception of risk regarding rule violation for individuals and organisations.

H3. Instances of violations linked to negative outcomes will increase the perception of risk associated with rule violation for individuals and organisations.

H4. The enforceability of regulations will positively impact the perception of risk of rule violation for individuals and organisations.

H5. The clarity of goals in rules and regulations will positively influence the perception of risk of violating those rules for individuals and organisations.

H6. Connectedness (referring to network connections or relationships) will positively influence the perception of risk of violating rules for individuals and organisations.

H7. A positive attitude towards rule-abiding behaviour will positively influence the perception of risk of violating rules for individuals and organisations.

H8. Subjective norms will positively influence the perception of risk of violating rules for individuals.

The theoretical model suggests the latent variables are typically unobservable constructs that underlie the observed behaviours related to privacy and security violations within an organisation. In assessing the latent variables it was grouped into Violation Coupling, Communication Structures, Enforceability, Goal Clarity of Rules, Rule Connectedness, Subjective Norms with the dependant variable being Attitude towards Behaviour. The dependent variables typically represent observable manifestation of privacy and security violations within the organisation.

The structural model was evaluated using Partial Least Squares Structural Equation Modelling (PLS-SEM). In assessment of the model outer loading relevance testing removed variables below the outer loading (0.40) and addressed any issues in data, outliers or unengaged respondents. By examining the Variance Inflation Factor (VIF) values of all sets of constructs in the structural model to check for collinearity issues (Hair Jr. et al., 2021).

$$VIF\text{j} = \frac{1}{1 - R_j^2}$$

$$VIFj = \frac{1}{1 - 0.765} = \frac{1}{0.235} \approx 4.255$$

As the results presented in table 10 all VIF values are below the threshold of approximately 4.255, it is then concluded that multicollinearity may not be a significant issue.

	Attitude towards Behaviour	Communication Structures	Enforceability	Goal Clarity of Rules	Rule Connectedness	Subjective Norms	Violation Coupling
Attitude towards Behaviour							
Communication Structures	1.359						
Enforceability	1.656						
Goal Clarity of Rules	2.564						

Rule Connectedness	2.782						
Subjective Norms	1.343						
Violation Coupling	1.607						

Table 10. VIF Values in the Structural Model

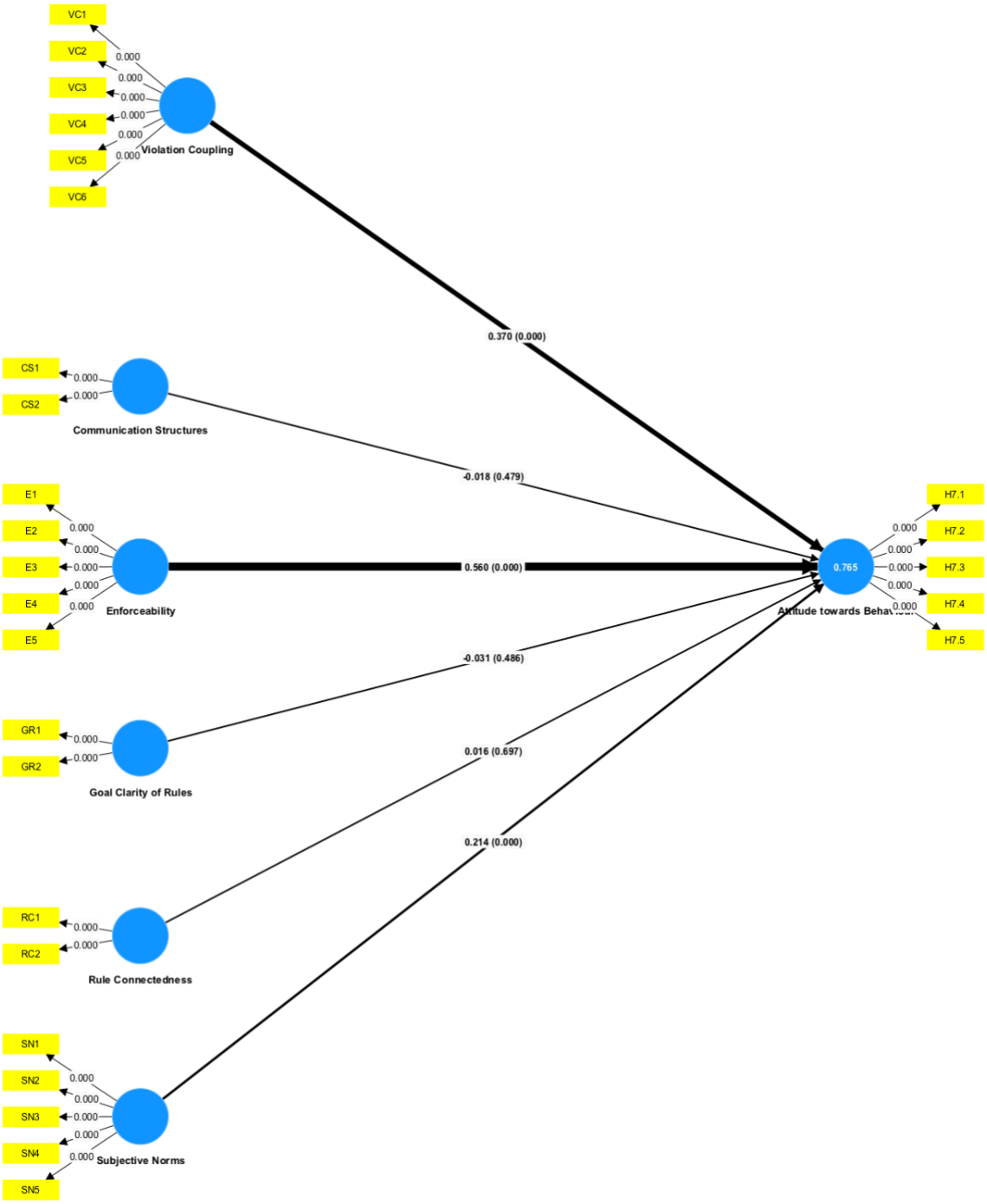


Figure 12. Bootstrapping p values in the Modelling Window

	Original sample (O)	Sample mean (M)	Standard deviation (STDEV)	T statistics (|O/STDEV|)	P values
Communication Structures -> Attitude towards Behaviour	-0.018	-0.019	0.025	0.709	0.479
Enforceability -> Attitude towards Behaviour	0.560	0.559	0.025	22.040	0.000
Goal Clarity of Rules -> Attitude towards Behaviour	-0.031	-0.028	0.044	0.697	0.486
Rule Connectedness -> Attitude towards Behaviour	0.016	0.015	0.041	0.389	0.697
Subjective Norms -> Attitude towards Behaviour	0.214	0.215	0.028	7.767	0.000
Violation Coupling -> Attitude towards Behaviour	0.370	0.368	0.029	12.836	0.000

Table 11. Path Coefficients

The assessment of Path coefficients for the relationship between the various constructs and 'Attitude towards Behaviour' as per results in Table 10 and visually represented in figure 12. The coefficient is negative for 'Communication Structures' and 'Goal Clarity of Rules', indicating a negative relationship, albeit very weak. The T statistic (|O/STDEV|) is 0.709 and 0.697 respectively, suggesting a small effect size. The p-value is 0.479 and 0.486, indicating that the relationship is not statistically significant. 'Enforceability', 'Rule Connectedness', 'Subjective Norms', 'Violation Coupling' coefficient is positive, indicating a positive relationship. The T statistic suggesting a small to large effect size and the p-value indicates that the relationship is statistically significant except for Rule Connectedness.

	Original sample (O)	Sample mean (M)	Bias	2.5%	97.5%
Communication Structures -> Attitude towards Behaviour	-0.018	-0.019	-0.001	-0.065	0.035
Enforceability -> Attitude towards Behaviour	0.560	0.559	-0.001	0.514	0.613
Goal Clarity of Rules -> Attitude towards Behaviour	-0.031	-0.028	0.003	-0.122	0.053
Rule Connectedness -> Attitude towards Behaviour	0.016	0.015	-0.001	-0.062	0.097
Subjective Norms -> Attitude towards Behaviour	0.214	0.215	0.001	0.160	0.268
Violation Coupling -> Attitude towards Behaviour	0.370	0.368	-0.002	0.311	0.424

Table 12. Percentile Confidence Intervals (with Bias Correction) for the Path Coefficients

Enforceability, subjective norms, and violation coupling demonstrate statistically significant positive relationships with attitude towards behaviour, while communication structures, goal clarity of rules, and rule connectedness show non-significant relationshipsas per table 12.

	R-square	R-square adjusted
Attitude towards Behaviour	0.765	0.761

Table 13. R squared

The R squared value is in excess of 0.75 as shown in Table 13 which indicates the substantial explanatory power of the model.

	Attitude towards Behaviour	Communication Structures	Enforceability	Goal Clarity of Rules	Rule Connectedness	Subjective Norms	Violation Coupling	Comment
Attitude towards Behaviour								
Communication Structures	0.001							Small effect
Enforceability	0.805							Large effect
Goal Clarity of Rules	0.002							Small effect
Rule Connectedness	0.000							Small effect
Subjective Norms	0.145							Medium effect
Violation Coupling	0.361							Large effect

Table 14. F Effect Sizes

Table 14 demonstrates the effect size of each construct (Cohen, 1988). Enforceability and violation coupling exhibit large effects on attitude towards behaviour, subjective norms demonstrate a medium effect, while communication structures, goal clarity of rules, and rule connectedness show small effects.

$$f^2 = \frac{R^2_{included} - R^2_{excluded}}{1 - R^2_{included}}$$

	Q^2predict	PLS-SEM_RMSE	PLS-SEM_MAE	LM_RMSE	LM_MAE	Relevance Comment
H7.1	0.233	0.447	0.332	0.283	0.224	Moderate Predictive
H7.2	0.317	0.541	0.415	0.319	0.258	Moderate Predictive
H7.3	0.290	0.586	0.416	0.319	0.251	Moderate Predictive
H7.4	0.502	0.521	0.357	0.226	0.163	Strong Predictive
H7.5	0.630	0.436	0.351	0.199	0.146	Strong Predictive

Table 15. PLSpredict Results Report

Table 15 represents Stone-Geisser's Q^2 value (GEISSER, 1974; Stone, 1974) which indicate the path models predictive relevance for the endogenous construct. Q^2 values indicate the proportion of variance explained by the model, and they suggest that the model has moderate to strong predictive power across the different hypotheses.

$$q^2 = \frac{Q^2_{included} - Q^2_{excluded}}{1 - Q^2_{included}}$$

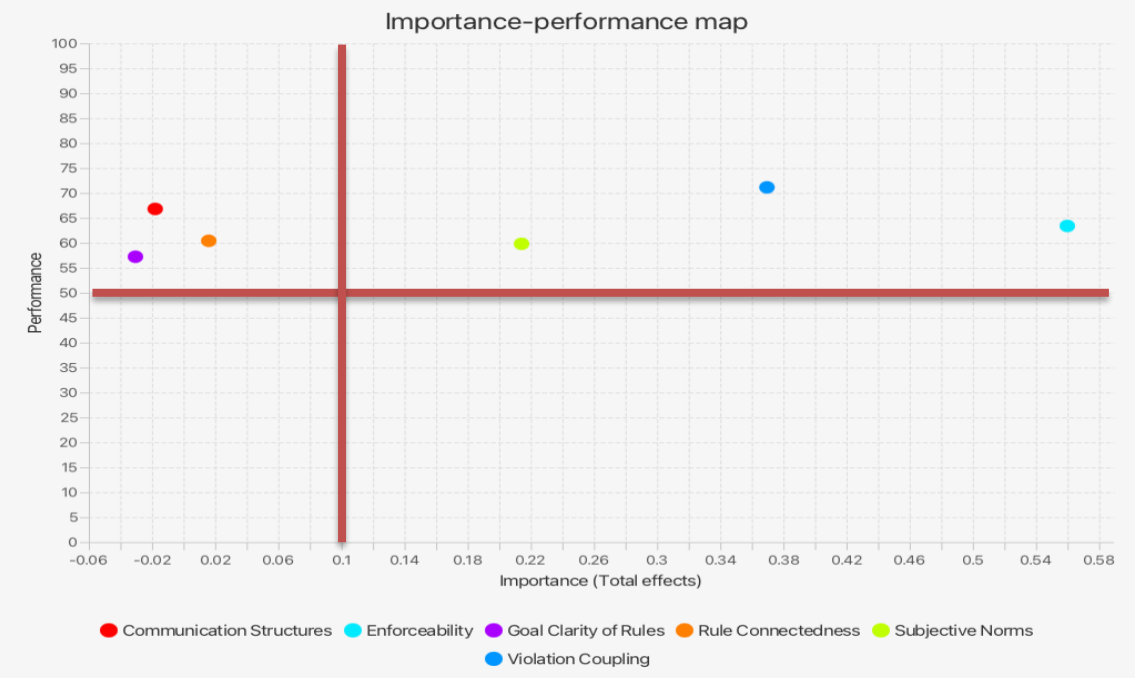


Figure 13. Importance Performance Map Analysis (IPMA)

Figure 13 presents the graphical representation of the Importance Performance Map Analysis (Martilla & James, 1977). The graph demonstrates which constructs should prioritise.

$$\mathcal{X}_{Scaled} = \frac{\mathcal{X} - \mathcal{X}_{min}}{\mathcal{X}_{max} - \mathcal{X}_{min}}$$

	Attitude towards Behaviour	Communication Structures	Enforceability	Goal Clarity of Rules	Rule Connectedness	Subjective Norms	Violation Coupling
Attitude towards Behaviour							
Communication Structures	-0.018						
Enforceability	0.560						
Goal Clarity of Rules	-0.031						
Rule Connectedness	0.016						
Subjective Norms	0.214						
Violation Coupling	0.370						

Table 16. Total Effects

$$T_{EX \to Y} = \beta_{X \to Y} + \sum_k (\beta_{X \to k} \times \beta_{k \to Y})$$

The total effect as depicted in Table 16 shows Enforceability has the strongest total effect on attitude towards behaviour(0.560), followed by violation coupling (0.370) and Subjective Norms (0.214).

4.6 Regression Analysis

The regression analysis illustrated in Table 17 provides insights into the distribution of variability within the dependent variable, which is the variable under prediction or explanation. The Total Sum of Squares reflects the entirety of this variability, with a value of 363.000 in this instance. The Error Sum of Squares signifies the portion of variability within the dependent variable that remains unaccounted for by the

regression model. Essentially, it quantifies the variance between observed values and those predicted by the model, with a calculated value of 85.378.

Conversely, the Regression Sum of Squares captures the variability within the dependent variable that can be attributed to the regression model. These metric gauges the efficacy of the independent variables in forecasting the dependent variable. Degrees of Freedom represent the quantity of independent data points available for estimating a parameter, while Mean Square provides an average measure of variability by dividing the sum of squares by its respective degrees of freedom. The F-statistic, with a value of 192.934 in this context, delineates the ratio between the mean square of the regression and that of the error. It serves as a crucial indicator of whether the variability elucidated by the regression model significantly exceeds that left unexplained.

The associated P-value offers insights into the statistical significance of the F-statistic. A low P-value, typically below 0.05, implies that the regression model possesses substantial explanatory power concerning the variance within the dependent variable. In summary, the analysis indicates that the regression model collectively holds significance ($p < 0.05$), signifying the presence of at least one independent variable with a non-zero coefficient. Furthermore, the model demonstrates a notable capability in elucidating variability within the dependent variable, as underscored by the elevated F-value.

	Sum square	**df**	**Mean square**	**F**	**P value**
Total	363.000	362	0.000	0.000	0.000
Error	85.378	356	0.240	0.000	0.000
Regression	277.622	6	46.270	192.934	0.000

Table 17. ANOVA

The coefficient (Table 18) implies that with each incremental unit rise in the Goal Clarity of Rules independent variable (IV), the dependent variable (DV) diminishes by 0.031 units. However, this coefficient lacks statistical significance given that the p-value exceeds 0.05. Consequently, Goal Clarity of Rules appears to exert no significant influence on the DV. Similarly, akin to the prior variable, Rule Connectedness does not demonstrate a statistically significant impact on the DV, as its associated p-value surpasses 0.05. In contrast, Subjective Norms yields a substantial positive effect on the DV. For every unit increase in the Subjective Norms IV, the DV escalates by 0.214 units. Notably, this variable exhibits a remarkably low p-value (0.000), signifying robust statistical significance. Conversely, resembling the first two variables, Communication Structures fail to manifest a statistically significant impact on the DV.

Conversely, Enforceability wields a highly significant positive influence on the DV. Each unit augmentation in the Enforceability IV corresponds to a 0.560 unit elevation in the DV. Similarly, Violation Coupling also exerts a notably positive and statistically significant impact on the DV, with each unit increase in the Violation Coupling IV correlating to a 0.370 unit augmentation in the DV. The intercept denotes the anticipated value of the DV when all independent variables are zero. In this instance, it lacks statistical significance, which aligns with typical expectations. Overall, Subjective Norms, Enforceability, and Violation Coupling appear to be significant predictors of the dependent variable, whereas Goal Clarity of Rules, Rule Connectedness, and Communication Structures do not show statistically significant effects.

	Unstandardized coefficients	Standardized coefficients	SE	T value	P value	2.5 %	97.5 %
LV scores - Goal Clarity of Rules	-0.031	-0.031	0.041	0.742	0.458	-0.111	0.050
LV scores - Rule Connectedness	0.016	0.016	0.043	0.371	0.711	-0.068	0.100
LV scores - Subjective Norms	0.214	0.214	0.030	7.186	0.000	0.155	0.273
LV scores - Communication Structures	-0.018	-0.018	0.030	0.602	0.548	-0.077	0.041
LV scores - Enforceability	0.560	0.560	0.033	16.925	0.000	0.495	0.625
LV scores - Violation Coupling	0.370	0.370	0.033	11.339	0.000	0.305	0.434
Intercept	-0.000	0.000	0.026	0.000	1.000	-0.051	0.051

Table 18. Coefficients

The results of the structural equation model provide a comprehensive overview of cybersecurity perspectives for protecting intangible commodities in financial institutions in South Africa and the validity of the theoretical model was tested using data collected (n = 363). Overall, the hypothesised model was well-fitted with the observed model.

4.7 Conclusion

Demographic analysis revealed a predominantly male representation (69.7%), with the majority falling within the age group of 35 to 44 years (51.52%). The banking sector accounted for the highest response rate (78.79%), followed by credit rating agencies (12.67%). Notably, many respondents reported more than 10 years of experience in the industry (90.91%). Reliability and validity assessments were conducted to ensure the robustness of the constructs used in the study. The analysis indicated acceptable reliability, with Cronbach's alpha values exceeding 0.7 for all constructs. Additionally, convergent validity was confirmed, with average variance extracted values surpassing 0.5 for most constructs.

Factor analysis provided insights into respondents' perceptions of the constructs, with generally positive responses observed across various dimensions. Hypothesis testing using Partial Least Squares Structural Equation Modeling (PLS-SEM) revealed that the theoretical model, encompassing latent variables such as Violation Coupling, Communication Structures, Enforceability, Goal Clarity of Rules, Rule Connectedness, and Subjective Norms, along with the dependent variable Attitude towards Behaviour, was supported by the empirical data. The structural model demonstrated significant positive relationships between Enforceability, Subjective Norms, Violation Coupling, and Attitude towards Behaviour. Communication Structures, Goal Clarity of Rules, and Rule Connectedness showed non-significant relationships with Attitude towards Behaviour as depicted in Table 19.

Objective	**Hypothesis**	**Results**	**Interpretation**
Identify the key cybersecurity controls relevant to protecting intangible commodities.	The perceived risk of violating a privacy or cybersecurity rule negatively affects the likelihood of a privacy or security rule violation aimed at safeguarding intangible commodities.	Standardised coefficient of 0.370 with a p-value of 0.000	Supported
	Instances of violations linked to negative outcomes will increase the perception of risk associated with rule violation for individuals and organisations.	Standardised coefficient of 0.016 with a p-value of 0.711	Not supported
	Connectedness (referring to network connections or relationships) will positively influence the perception of risk of violating rules for individuals and organisations.	Standardised coefficient of 0.016 with a p-value of 0.711	Not supported
	Subjective norms will positively influence the perception of risk of violating rules for individuals.	Standardised coefficient of 0.214 with a p-value of 0.000	Supported
Evaluate the feasibility and viability of adopting global frameworks and standards in the context of South Africa's connected world.	Both formal and informal communication structures that promote regulatory compliance will heighten the perception of risk regarding rule violation for individuals and organisations.	Standardised coefficient of -0.018 with a p-value of 0.548	Not supported
	The enforceability of regulations will positively impact the perception of risk of rule violation for individuals and organisations.	Standardised coefficient of 0.560 with a p-value of 0.000	Supported

Develop a monitoring and measurement framework to assess the effectiveness of current cybersecurity controls for safeguarding intangible commodities.	The clarity of goals in rules and regulations will positively influence the perception of risk of violating those rules for individuals and organisations.	Standardised coefficient of -0.031 with a p-value of 0.458	Not supported
	A positive attitude towards rule-abiding behaviour will positively influence the perception of risk of violating rules for individuals and organisations.	Standardised coefficient of 0.000 with a p-value of 1.000	Not supported

Table 19. Summary of Hypothesis and Results

Regression analysis further elucidated the distribution of variability within the dependent variable. The regression model collectively held significance, indicating that at least one independent variable had a non-zero coefficient and demonstrated notable explanatory power regarding the variance within the dependent variable.

CHAPTER 5. INTEPRETATION OF THE RESULTS

5.1 Introduction

This chapter presents a summary of the research results, conclusions, and recommendations. The purpose of the research was to provide a comprehensive overview of cybersecurity perspectives for protecting intangible commodities in financial institutions in South Africa. The research report extends this area of study by delving into Selective Organisational Information Privacy and Security Violations (SOIPSV). This concept revolves around organisations deliberately bypassing privacy and security protocols for particular objectives in securing intangible commodities (Wall et al., 2015). This could involve accessing, sharing, or using sensitive information in ways that are not compliant with ethical, legal, or industry standards. Financial institutions are regarded as critical sources that house significantly large volumes of intangible assets.

5.2 Hypothesis Summary Results

5.2.1 *The perceived risk of violating a privacy or cybersecurity rule negatively affects the likelihood of a privacy or security rule violation aimed at safeguarding intangible commodities.*

The perception of risk associated with violating privacy or cybersecurity rules negatively affects the likelihood of actual rule violations, supporting the hypothesis. This statement suggests that if individuals perceive a high risk associated with breaking privacy or cybersecurity rules, they are less likely to actually violate those rules. Essentially, it means that people are more cautious when they believe there are serious consequences for their actions in terms of privacy or cybersecurity breaches. This has implications for policymaking and organisational practices because it indicates that strengthening

perceptions of risk could be an effective strategy for deterring rule violations and promoting compliance.

5.2.2 *Instances of violations linked to negative outcomes will increase the perception of risk associated with rule violation for individuals and organisations.*

There is no significant evidence to support the hypothesis that instances of violations linked to negative outcomes increase the perception of risk associated with rule violation for individuals and organisations. It suggests that the relationship between instances of violations and the perception of risk might not be as straightforward as initially thought. Without strong evidence linking violations to increased risk perception, it could imply several things.

People and organisations might not perceive rule violations as inherently risky. Other factors could influence their perception, such as the severity of consequences or the frequency of violations. Violations might be so common or culturally accepted within certain contexts that they don't significantly impact risk perception. In such cases, individuals or organisations might become desensitized to the associated risks. There could be confounding variables that haven't been accounted for in the research. These variables might mediate or moderate the relationship between violations and risk perception, making it challenging to detect a clear pattern.

People and organisations might vary in how they perceive and respond to violations. Factors such as personality traits, past experiences, or organisational culture could influence risk perception independently of violation instances. The absence of significant evidence could also stem from limitations in the research design or measurement techniques used. Perhaps the studies lacked sufficient statistical power, or the measures of risk perception were not sensitive enough to detect changes.

5.2.3 *Connectedness (referring to network connections or relationships) will positively influence the perception of risk of violating rules for individuals and organisations.*

There is no significant evidence to support the hypothesis that connectedness positively influences the perception of risk of violating rules for individuals and organisations. Understanding how individuals and organisations perceive risk is crucial for designing effective strategies for risk management and compliance. Since this hypothesis isn't supported, it could indicate that other factors play a more dominant role in shaping perceptions of risk.

This finding could lead to investigations into alternative factors that influence risk perception. It's possible that social, cultural, or psychological factors have a stronger impact on how people and organisations perceive risks associated with rule violations. Exploring these factors could provide valuable insights into decision-making processes related to compliance and risk management.

From a practical standpoint, it raises questions about the effectiveness of certain policies and strategies aimed at promoting compliance and deterring rule violations (Palko et al., 2023). If the perceived risk associated with rule violations remains unaffected by instances of negative outcomes, alternative approaches may be needed to incentivise compliance and mitigate risk effectively.

5.2.4 *Subjective norms will positively influence the perception of risk of violating rules for individuals.*

Understanding that subjective norms positively influence the perception of risk of violating rules for individuals is important for several reasons. If subjective norms influence how individuals perceive the risk of violating rules, then it can help predict their behaviour. Individuals who perceive a higher risk of violating rules due to social pressures may be more likely to conform to those rules (Ajzen, 1991). This finding can

inform policymakers and institutions about the importance of considering subjective norms when designing rules and regulations. Simply imposing rules without considering social influences may not be as effective in promoting compliance.

Knowing that subjective norms play a role in risk perception can guide intervention strategies aimed at promoting rule compliance. For example, interventions could focus on changing social norms to align with desired behaviours, thus influencing individuals' risk perceptions. Understanding the impact of subjective norms on risk perception sheds light on the broader social dynamics at play in rule adherence. It highlights the role of social influence in shaping individual attitudes and behaviours towards rule compliance. Recognising the influence of subjective norms on risk perception contributes to a more comprehensive understanding of human behaviour in social contexts and can inform strategies aimed at promoting compliance with rules and regulations (Alanazi et al., 2022).

5.2.5 *Both formal and informal communication structures that promote regulatory compliance will heighten the perception of risk regarding rule violation for individuals and organisations.*

Organisations might need to reassess their communication structures to determine if they are effectively conveying the importance of regulatory compliance. It could be that the current methods aren't as impactful as initially thought. The absence of a correlation between communication structures and perception of risk might indicate that other factors play a more significant role in shaping individuals' and organisations' attitudes toward rule violation. These factors could include leadership behaviour, organisational culture, or external pressures.

Organisations may need to adapt their compliance strategies based on emerging insights. If communication structures alone don't effectively mitigate the perception of risk, alternative approaches may be necessary. If communication isn't effectively

reducing the perception of risk, emphasis might need to be placed on enforcement mechanisms and consequences for rule violations.

5.2.6 *The enforceability of regulations will positively impact the perception of risk of rule violation for individuals and organisations.*

The enforceability of regulations positively impacts the perception of risk of rule violation for individuals and organisations, supporting the hypothesis. The significance of regulations being enforceable lies in their ability to influence how seriously individuals and organisations perceive the risk of violating those rules. When regulations are effectively enforced, it creates a tangible consequence for non-compliance, which can act as a deterrent. This, in turn, supports the hypothesis that the perception of risk associated with breaking rules is heightened when there's a likelihood of enforcement. Consequently, individuals and organisations are more likely to adhere to regulations when they believe there are real consequences for not doing so. This can lead to better compliance overall, which is crucial for maintaining order, safety, and fairness within society or specific sectors.

5.2.7 *A positive attitude towards rule-abiding behaviour will positively influence the perception of risk of violating rules for individuals and organisations.*

The relationship between attitude and risk perception might not be as straightforward as previously assumed. Organisations might need to reassess their strategies for promoting rule-abiding behaviour if they rely solely on fostering positive attitudes without considering their impact on risk perception. Researchers and practitioners might need to explore other factors that influence risk perception and rule compliance, such as organisational culture, leadership, or situational variables.

5.2.8 *The clarity of goals in rules and regulations will positively influence the perception of risk of violating those rules for individuals and organisations.*

It suggests that other factors may play a more prominent role in determining how individuals and organisations perceive the risk of violating rules. The lack of evidence doesn't necessarily mean the hypothesis is false, it could indicate a gap in understanding or methodological limitations in existing studies. Further research may be needed to explore this relationship more thoroughly. If clarity of goals in rules and regulations doesn't significantly impact risk perception, it prompts consideration of other factors that might be more influential. This could include the severity of potential consequences, the likelihood of enforcement, or cultural norms surrounding rule compliance.

In summary, while some hypotheses are supported, such as the impact of perceived risk and subjective norms on behaviour, others are rejected due to lack of significant evidence, such as the influence of communication structures and clarity of goals. These findings provide valuable insights into factors influencing the perception of risk and behaviour regarding privacy and cybersecurity rule violations.

5.3 Conclusion

5.3.1 *Identify the key cybersecurity controls relevant to protecting intangible commodities*

The first objective seeked to understand what are key controls for protecting intangible commodities. Based on the statistical analysis completed, the data suggests that subjective norms and violation coupling have significant impacts on attitudes towards behaviour in cybersecurity, as indicated by their low p-values ($p < 0.05$). However, the rule connectedness does not show a significant impact.

Subjective norms as adapted from (Ajzen, 1991) and described by (Rebecca Sansom, 2021) encompass social pressures, encompassing both the perceived expectations of others and the significance an individual assigns to those expectations. Subjective norms, constituting the social pressures influencing an individual's actions, as per (Anastasia & Santoso, 2020), can arise from various sources such as parents, colleagues, and media. These pressures significantly influence an individual's inclination to safeguard Intangible commodities for personal gain. Violation coupling refers to the degree to which an individual's perception of violations of cybersecurity practices or policies is linked to their attitude towards adhering to those practices or policies. In simpler terms, it measures how closely a person associates breaking cybersecurity rules with their attitude towards following those rules.

5.3.2 *Evaluate the feasibility and viability of adopting global frameworks and standards in the context of South Africa's connected world.*

The analysis of the data presented in chapter 4 suggests that while there's no significant impact of communication structures, enforceability of standards has a substantial and positive influence. This indicates that focusing on enforceability may be more critical than communication structures when considering the adoption of global frameworks and standards in South Africa's connected world.

In the realm of technology and Selective Organisational Information Privacy and Security Violations Management (SOIPSVM), enforceability begins with transparency. Often, individuals lack insight into whether the sites they visit honour their opt-outs or privacy preferences (Zimmeck et al., 2023). Presently, non-compliant sites can operate without detection, posing minimal risk of exposure. Therefore, it's crucial to enhance the visibility of how sites handle Global Privacy Control (GPC) and other privacy signals (Zimmeck et al., 2023). Transparently disclosing a site's practices serves as a powerful incentive for compliance.

In the present era (Alshudukhi et al., 2023), countless devices exchange confidential personal and business data, posing a threat to privacy and undermining confidence in the system if left unregulated. With the rapid pace of innovation, security concerns are frequently overlooked, with functionality taking precedence as the primary driving force. Challenges include non-adoption, budget constraints, and staff readiness for emerging technologies (Farid et al., 2023). Regulators, through the establishment and enforcement of rules, aim to influence the behaviour of managers and employees within regulated organisations (Coglianese, 2024). This influence is directed towards reducing risks and addressing various regulatory issues, including those related to information privacy and security.

5.3.3 *Develop a monitoring and measurement framework to assess the effectiveness of current cybersecurity controls for safeguarding intangible commodities.*

According to SORVM, rules emphasizing procedures over desired outcomes are believed to reduce perceptions of risk. This proposition stems from the idea that procedures enable organisations to demonstrate compliance to regulatory bodies, even if organisational behaviours deviate from the intended outcomes of the rule (Wall et al., 2015). Goal clarity is the degree to which a rule clearly defines objectives, minimising the possibility of alternative interpretations, and offers guidance on achieving these objectives.

Within the implemented information security policy, it is incumbent upon every organisation to consistently assess the risks and threats posed to the data under its purview. Entrepreneurs have the capability to categorise their systems according to the magnitude of risk linked to potential security incidents (Palko et al., 2023). The risk assessment process adheres to an iterative approach and encompasses three fundamental tasks.

1. Collecting data and policies

2. Performing risk evaluations based on their scrutiny, and
3. Furnishing decision-making support.

The researchers (Chen & Yuan, 2022) discovered that optimism bias resulted in a reduced perception of information security risks, while the absence of knowledge regarding those risks did not notably impact the perceived threat. Conducting regular assessments of the effectiveness of cybersecurity controls against the established KPIs will provide guidance on the progress and adoption of controls implemented.

Selective Organisational Information Privacy and Security Violations Management (SOIPSVM) complements existing cybersecurity frameworks. SOIPSVM offers a granular approach to managing privacy and security violations within an organisation. While traditional cybersecurity frameworks provide overarching guidelines, SOIPSVM allows the organisations to focus on specific instances of violations and tailor responses accordingly. SOIPSVM further emphasizes understanding and addressing the behavioural aspects of security violations. By considering how individuals within an organisation perceive and respond to security threats. Organisations can incorporate SOIPSVM principles into their existing policies and procedures, enhancing the overall cybersecurity posture.

SOIPSVM extends and encourages a continuous improvement mindset towards cybersecurity. By analysing and learning from past security incidents, organisations can refine their strategies and strengthen their defenses over time. Helps organisations take a comprehensive approach to risk management by addressing both intentional and unintentional security violations. By considering a wide range of potential threats and vulnerabilities which enhances the resilience of cybersecurity frameworks used.

Overall, SOIPSVM enhances existing cybersecurity frameworks by providing a focused, behaviour-centric approach to managing privacy and security violations within organisations. By incorporating SOIPSVM principles, organisations can strengthen their cybersecurity posture and better protect their sensitive information and assets.

CHAPTER 6. CONCLUSION AND RECOMMENDATIONS

6.1 Introduction

The interpretation of the results obtained from the research, aimed to provide a comprehensive overview of cybersecurity perspectives for protecting intangible commodities in financial institutions in South Africa. Utilising the Selective Organisational Information Privacy and Security Violations Model (SOIPSVM), the research analysed various factors within South Africa's socio-economic, technological, and regulatory landscape. A quantitative approach was employed receiving 519 responses, targeted at technology professionals or leaders with influence in cybersecurity within the financial services industry.

6.2 Conclusion

The research objectives were systematically addressed through hypothesis testing and data analysis. Hypotheses related to the perceived risk of violating privacy or cybersecurity rules, communication structures promoting regulatory compliance, enforcement of regulations, clarity of rules and regulations, connectedness, positive attitudes towards rule-abiding behaviour, and subjective norms were tested. The analysis emphasizes the critical role of enforceability of standards in driving compliance with cybersecurity measures, suggesting that efforts to enhance enforceability may be more critical than focusing solely on communication structures. Transparency in handling privacy preferences is identified as a crucial factor for promoting compliance with global privacy standards, further emphasizing the need for clear and transparent communication regarding data handling practice.

It was noted through the analysis and interpretation of results that Selective Organisational Information Privacy and Security Violations Management (SOIPSVM)

complements existing cybersecurity frameworks by offering a focused approach to managing and mitigating privacy and security risks within organisations. While traditional cybersecurity frameworks provide comprehensive guidelines and best practices for safeguarding digital assets, SOIPSVM offers specific strategies for addressing organisational behaviours that may lead to privacy and security breaches. By focusing on the management of intentional violations and non-compliance with security policies, SOIPSVM enhances the effectiveness of existing cybersecurity frameworks by targeting internal factors that may undermine security measures.

6.2.1 *Identify the key cybersecurity controls relevant to protecting intangible commodities*

The perceived risk of violating privacy or cybersecurity rules significantly impacts the likelihood of actual rule violations, indicating a crucial link between risk perception and compliance behaviour. When individuals and organisations perceive a high risk associated with breaking such rules, they exhibit greater caution, thus deterring potential violations and promoting adherence to regulations aimed at safeguarding intangible commodities.

Instances of violations linked to negative outcomes do not necessarily increase the perception of risk associated with rule violation, challenging the straightforward relationship between violation instances and risk perception. This suggests a more complex interplay of factors influencing risk perception, including the complexity of perception, normalisation of violations, confounding variables, individual differences, and methodological limitations.

Moreover, the hypothesis that connectedness positively influences the perception of risk of violating rules for individuals and organisations lacks significant evidence, highlighting the need to explore alternative factors such as social, cultural, or psychological influences on risk perception. This underscores the importance of

considering diverse factors in designing effective strategies for risk management and compliance.

On the other hand, subjective norms play a crucial role in shaping risk perception, with individuals influenced by social pressures more likely to conform to rules. Understanding this influence can inform policymakers and institutions about the importance of considering subjective norms in rule design and intervention strategies aimed at promoting compliance.

In essence, recognising the multifaceted nature of risk perception and its influences on behavior is essential for developing comprehensive strategies to mitigate risks effectively and promote adherence to rules and regulations in the realm of privacy and cybersecurity. Further research into these dynamics can provide valuable insights into human behaviour in social contexts and inform targeted interventions to enhance compliance efforts.

6.2.2 *Evaluate the feasibility and viability of adopting global frameworks and standards in the context of South Africa's connected world.*

The effectiveness of communication structures in promoting regulatory compliance appears to be nuanced, with formal and informal methods potentially yielding differing results. While it was initially assumed that robust communication would heighten the perception of risk regarding rule violation, the absence of a clear correlation suggests that other factors, such as leadership behaviour, organisational culture, or external pressures, may exert stronger influences on attitudes toward compliance.

Organisations must critically reassess their communication strategies to ensure they effectively convey the importance of regulatory compliance. If current methods prove inadequate in mitigating the perception of risk, alternative approaches may be necessary. Emphasizing enforcement mechanisms and consequences for violations

could supplement communication efforts, ensuring a comprehensive compliance strategy.

The hypothesis regarding the enforceability of regulations positively impacting the perception of risk finds support. Effective enforcement creates tangible consequences for non-compliance, acting as a deterrent and heightening the perceived risk of rule violation. Consequently, individuals and organisations are more inclined to adhere to regulations when they believe enforcement is likely, fostering better overall compliance and contributing to societal order, safety, and fairness within specific sectors.

While communication structures may require refinement, the enforceability of regulations emerges as a crucial factor in shaping perceptions of risk and promoting compliance. Organisational strategies should thus prioritise both clear communication and robust enforcement mechanisms to foster a culture of adherence to regulatory standards.

6.2.3 *Develop a monitoring and measurement framework to assess the effectiveness of current cybersecurity controls for safeguarding intangible commodities.*

While certain hypotheses regarding the influence of attitudes towards rule-abiding behavior and the clarity of goals in rules and regulations on risk perception were initially posited, the relationship between these factors and risk perception appears more complex than anticipated. The absence of significant evidence linking positive attitudes towards rule-abiding behavior to heightened risk perception suggests a need for organisations to reassess their strategies for promoting compliance. Relying solely on fostering positive attitudes may not effectively influence risk perception, prompting researchers and practitioners to explore alternative factors such as organisational culture, leadership, or situational variables that may have a more substantial impact.

The hypothesis regarding the clarity of goals in rules and regulations positively influencing risk perception lacks robust support. This suggests that other factors may play a more prominent role in determining how individuals and organisations perceive the risk of violating rules. Further research is warranted to explore this relationship more thoroughly and identify additional influential factors such as the severity of potential consequences, the likelihood of enforcement, or cultural norms surrounding rule compliance.

These findings provide valuable insights into the multifaceted nature of factors influencing risk perception and behavior regarding privacy and cybersecurity rule violations.

6.3 Recommendations

6.3.1 *Practice*

Organisations should prioritise efforts to enhance compliance with cybersecurity standards by focusing on enforceability and transparency in data handling practices (Harris & Martin, 2019). Providing comprehensive education and training programs on cybersecurity best practices can help improve awareness and understanding of the importance of compliance among employees and stakeholders (Mohammed, 2015).

Policymakers may need to reevaluate the emphasis placed on clarity of rules and regulations as a means of reducing risk perception. Instead, they might need to focus on other strategies to effectively communicate and enforce compliance. Organisations may need to reassess their approach to rule communication and enforcement (Poire & Dailey, 2006). If clarity of goals doesn't reduce risk perception, they may need to explore other avenues such as training, incentives, or organisational culture to promote compliance. In essence, while the lack of significant evidence challenges the assumption that clarity of goals influences risk perception, it opens avenues for deeper exploration

and consideration of alternative factors in understanding and addressing compliance behaviour.

Implementing a monitoring and measurement framework (Gordon et al., 2020) to assess the effectiveness of cybersecurity controls on an ongoing basis is essential for identifying areas for improvement and ensuring continued compliance with regulatory requirements. Collaboration among organisations and sharing of best practices can help strengthen cybersecurity efforts and promote a culture of compliance across industries. By implementing these recommendations, organisations can enhance their cybersecurity posture and better protect intangible commodities from security threats, ultimately contributing to a safer and more secure digital environment.

6.3.2 *Theoretical Contributions*

While the lack of significant evidence might seem discouraging, it also presents an opportunity for further exploration and refinement of theories regarding risk perception and rule violations. It suggests that there's more complexity to the relationship than previously understood, inviting researchers to delve deeper into understanding the nuances at play.

Moving forward, a comprehensive understanding of these dynamics will be essential for developing effective strategies to promote compliance and mitigate risks effectively.

6.4 Limitations of the Study

While your research provides valuable insights into cybersecurity perspectives for protecting intangible commodities in financial institutions in South Africa, there are some limitations and considerations to be aware of. The study focused on technology professionals or leaders in the financial services industry, potentially excluding perspectives from other relevant stakeholders. This bias might limit the generalisability of the findings to a broader audience within and outside the industry.

The reliance on self-reported data in a quantitative approach could introduce response bias. Participants may provide socially desirable responses or inaccuracies, impacting the reliability and validity of the results. The study focuses on South Africa, and the findings may not be directly applicable to other regions due to unique socio-economic, cultural, and regulatory contexts. The rapidly evolving nature of cybersecurity threats and technologies may render the study's findings time sensitive. The landscape may have changed since the data collection, affecting the relevance of the results.

While the Selective Organisational Information Privacy and Security Violations Model (SOIPSVM) offers a focused approach, relying solely on one model might overlook other relevant frameworks or aspects that contribute to cybersecurity.

6.5 Recommendations for Future Studies

Further research recommendations in the realm of SOIPSVM should include conducting empirical studies to validate the effectiveness of SOIPSVM strategies in real-world organisational settings (Sarah Slight et al., 2011). This could involve case studies or longitudinal studies tracking the implementation of SOIPSVM practices and their impact on privacy and security outcomes. Explore how SOIPSVM can be integrated into existing cybersecurity frameworks to provide a more comprehensive approach to risk management. This could involve developing guidelines or frameworks for incorporating SOIPSVM principles into established cybersecurity standards. Investigate the role of organisational culture in shaping attitudes towards privacy and security violations, and how SOIPSVM strategies can be tailored to address cultural factors that may influence compliance with security policies.

Explore the development of technological solutions to support SOIPSVM implementation, such as automated monitoring systems or decision support tools for identifying and addressing security violations. Examine the alignment of SOIPSVM practices with regulatory requirements and compliance standards and identify areas where SOIPSVM can help organisations meet regulatory obligations more effectively.

Further research into SOIPSVM can contribute to the development of more targeted and effective strategies for managing privacy and security risks within organisations, ultimately enhancing cybersecurity posture and protecting digital assets. By employing the SOIPSVM framework, stakeholders can make informed decisions and develop strategies to enhance cybersecurity readiness and resilience in South Africa's financial institutions.

REFERENCES

6 challenges to financial inclusion in South Africa. (2017, April 27). World Economic Forum. https://www.weforum.org/agenda/2017/04/financial-inclusion-south-africa/

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, *50*(2), 179–211. https://doi.org/10.1016/0749-5978(91)90020-T

Alanazi, M., Freeman, M., & Tootell, H. (2022). Exploring the factors that influence the cybersecurity behaviors of young adults. *Computers in Human Behavior*, *136*, 107376. https://doi.org/10.1016/j.chb.2022.107376

Albshaier, L., Almarri, S., & Hafizur Rahman, M. M. (2024). A Review of Blockchain's Role in E-Commerce Transactions: Open Challenges, and Future Research Directions. *Computers*, *13*(1), Article 1. https://doi.org/10.3390/computers13010027

Aliyu, A., Maglaras, L., He, Y., Yevseyeva, I., Boiten, E., Cook, A., & Janicke, H. (2020). A Holistic Cybersecurity Maturity Assessment Framework for Higher Education Institutions in the United Kingdom. *Applied Sciences*, *10*(10), Article 10. https://doi.org/10.3390/app10103660

Alsharida, R. A., Al-rimy, B. A. S., Al-Emran, M., & Zainal, A. (2023). A systematic review of multi perspectives on human cybersecurity behavior. *Technology in Society*, *73*, 102258. https://doi.org/10.1016/j.techsoc.2023.102258

Alshudukhi, K. S., Khemakhem, M. A., Eassa, F. E., & Jambi, K. M. (2023). An Interoperable Blockchain Security Frameworks Based on Microservices and Smart Contract in IoT Environment. *Electronics*, *12*(3), Article 3. https://doi.org/10.3390/electronics12030776

Alyami, A., Sammon, D., Neville, K., & Mahony, C. (2023). The critical success factors for Security Education, Training and Awareness (SETA) program effectiveness: A lifecycle model. *Information Technology & People*, *36*(8), 94–125. https://doi.org/10.1108/ITP-07-2022-0515

Amelia Ho. (2018). Roles of Three Lines of Defense for Information Security and Governance. *ISACA Journal*, *4*.

Anastasia, N., & Santoso, S. (2020). Effects of Subjective Norms, Perceived Behavioral Control, Perceived Risk, and Perceived Usefulness towards Intention to Use Credit Cards in Surabaya, Indonesia. *SHS Web of Conferences*, *76*, 01032. https://doi.org/10.1051/shsconf/20207601032

Asmundson, I. (2011, March). *What Are Financial Services?* Finance and Development | F&D. https://www.imf.org/external/pubs/ft/fandd/2011/03/basics.htm

Bagui, L., Lusinga, S., Pule, N., Tuyeni, T., Mtegha, C. Q., Calandro, E., Chigona, W., & von Solms, B. (2023). The impact of COVID-19 on cybersecurity awareness-raising and mindset in the southern African development community (SADC). *THE ELECTRONIC JOURNAL OF INFORMATION SYSTEMS IN DEVELOPING COUNTRIES*, *n/a*(n/a), e12264. https://doi.org/10.1002/isd2.12264

Bahiti, R., & Josifi, J. (2015). Towards a More Resilient Cyberspace: The Case of Albania. *Information & Security: An International Journal*, *32*, 120–130. https://doi.org/10.11610/isij.3210

Bora, A. (2017). Semantics of ruling: Reflective theories of regulation, governance and law. In *Society, Regulation and Governance* (pp. 15–37). Edward Elgar Publishing. https://www.elgaronline.com/edcollchap/edcoll/9781786438379/9781786438379.00008.xml

Brigit Helms. (2006). *Access for All: Building Inclusive Financial Systems*. https://openknowledge.worldbank.org/entities/publication/4608631f-9284-56b3-a65f-de86c8935e31

Chatman, J. A., & O'Reilly, C. A. (2016). Paradigm lost: Reinvigorating the study of organizational culture. *Research in Organizational Behavior*, *36*, 199–224. https://doi.org/10.1016/j.riob.2016.11.004

Chen, H., & Yuan, Y. (2022). The impact of ignorance and bias on information security protection motivation: A case of e-waste handling. *Internet Research*, *33*(6), 2244–2275. https://doi.org/10.1108/INTR-04-2022-0238

CIS Controls Version 8. (n.d.). CIS. Retrieved May 27, 2024, from https://www.cisecurity.org/controls/v8/

Clark, D. D. (2010). *Characterizing cyberspace: Past, present and future* [Working Paper]. © Massachusetts Institute of Technology. https://dspace.mit.edu/handle/1721.1/141692

COBIT | Control Objectives for Information Technologies. (n.d.). ISACA. Retrieved May 27, 2024, from https://www.isaca.org/resources/cobit

Coglianese, C. (2024). Rule Design: Defining the Regulator–Regulatee Relationship. In J.-C. Le Coze & B. Journé (Eds.), *The Regulator–Regulatee Relationship in High-Hazard Industry Sectors* (pp. 89–97). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-49570-0_10

Cohen, J. (1988). *Statistical power analysis for the behavioral sciences* (2nd ed). L. Erlbaum Associates.

Cronbach, L. J. (1949). *Essentials of psychological testing* (pp. xiii, 475). Harper.

CSF 2.0 Profiles. (2024). *NIST*. https://www.nist.gov/profiles-0

Demek, K. C., & Kaplan, S. E. (2023). Cybersecurity breaches and investors' interest in the firm as an investment. *International Journal of Accounting Information Systems*, *49*, 100616. https://doi.org/10.1016/j.accinf.2023.100616

Demmou, L., Stefanescu, I., & Arquié, A. (2019). *PRODUCTIVITY GROWTH AND FINANCE: THE ROLE OF INTANGIBLE ASSETS - A SECTOR LEVEL ANALYSIS ECONOMICS DEPARTMENT WORKING PAPERS No. 1547*.

Elliott, J., & Verkoren, C. (2022, February 11). *South Africa: Financial Sector Assessment Program-Financial System Stability Assessment*. https://www.imf.org/en/Publications/CR/Issues/2022/02/11/South-Africa-Financial-Sector-Assessment-Program-Financial-System-Stability-Assessment-513014

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

Farid, G., Warraich, N. F., & Iftikhar, S. (2023). Digital information security management policy in academic libraries: A systematic review (2010–2022). *Journal of Information Science*, 01655515231160026. https://doi.org/10.1177/01655515231160026

Financial Sector Regulation Act 9 of 2017. (n.d.). Retrieved July 27, 2023, from https://www.gov.za/sites/default/files/gcis_document/201708/4106022-8act9of2017finansectorregulationa.pdf

Fischer, E. A. (2016). *Cybersecurity Issues and Challenges: In Brief*.

Flick, U. (2013). *The SAGE Handbook of Qualitative Data Analysis*. SAGE.

Force, J. T. (2020). *Security and Privacy Controls for Information Systems and Organizations* (NIST Special Publication (SP) 800-53 Rev. 5). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-53r5

GEISSER, S. (1974). A predictive approach to the random effect model. *Biometrika*, *61*(1), 101–107. https://doi.org/10.1093/biomet/61.1.101

Glazer, E., & Yadron, D. (2014, October 2). J.P. Morgan Says About 76 Million Households Affected By Cyber Breach. *Wall Street Journal*. http://online.wsj.com/articles/j-p-morgan-says-about-76-million-households-affected-by-cyber-breach-1412283372

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

Goutam, R. K. (2015). Importance of Cyber Security. *International Journal of Computer Applications*, *111*(7), 14–17.

Grace Smith, McCann FitzGerald, & Anna-Marie Harty. (2008, April). *Finance-Magazine.com—Intellectual property protection for financial services*. http://www.finance-magazine.com/display_article.php?i=8295&ht=

Gulyás, O., & Kiss, G. (2023). Impact of cyber-attacks on the financial institutions. *Procedia Computer Science*, *219*, 84–90. https://doi.org/10.1016/j.procs.2023.01.267

Hair Jr., J. F., Hult, G. T. M., Ringle, C. M., Sarstedt, M., Danks, N. P., & Ray, S. (2021). *Partial Least Squares Structural Equation Modeling (PLS-SEM) Using R: A Workbook*. Springer Nature. https://doi.org/10.1007/978-3-030-80519-7

Harris, M. A., & Martin, R. (2019). Promoting Cybersecurity Compliance. In *Cybersecurity Education for Awareness and Compliance* (pp. 54–71). IGI Global. https://doi.org/10.4018/978-1-5225-7847-5.ch004

Henwood, R. D., u96195577@tuks.co.za, & Hlase, E. P. (2018). *The Securitisation of cyberspace in South Africa: The tension between national security and civil liberties continues*. https://repository.up.ac.za/handle/2263/68025

Hillman, A. J., Withers, M. C., & Collins, B. J. (2009). Resource Dependence Theory: A Review. *Journal of Management*, *35*(6), 1404–1427. https://doi.org/10.1177/0149206309343469

Hunton, P. (2011). A rigorous approach to formalising the technical investigation stages of cybercrime and criminality within a UK law enforcement environment. *Digital Investigation*, *7*(3), 105–113. https://doi.org/10.1016/j.diin.2011.01.002

International Organization for Standardization. (2018, February). *ISO/IEC 27000:2018*. https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27000:ed-5:v1:en

International Organization for Standardization. (2022a, March). *ISO/IEC 27002:2022*. https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27002:ed-3:v2:en

International Organization for Standardization. (2022b, October). *ISO/IEC 27001:2022*. https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27001:ed-3:v1:en

International Organization for Standardization. (2023, June). *ISO/IEC 27032:2023*. https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27032:ed-2:v1:en

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, *80*(5), 973–993. https://doi.org/10.1016/j.jcss.2014.02.005

Jeffrey D. Wall, Paul Benjamin Lowry, & Jordan B. Barlow. (2016, January). *Organizational Violations of Externally Governed Privacy and Security Rules: Explaining and Predicting Selective Violations under Conditions of Strain and Excess - ProQuest*. https://www.proquest.com/docview/1764090093?parentSessionId=BwL9HU14

tRdS4YRXQmUAYarZGNwlEWfOGQ9MsChaE7U%3D&pq-origsite=summon&accountid=15083&sourcetype=Scholarly%20Journals

John Ward Creswell & John David Creswell. (2022, November). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches | Online Resources*. https://edge.sagepub.com/creswellrd6e?_gl=1*10jfm4q*_ga*MTQ4Nzc0NjYwNy4xNjg3MTk0MDY4*_ga_60R758KFDG*MTY4NzE5NDA2OC4xLjEuMTY4NzE5NDc3My41OS4wLjA.*_ga_RK7MQ5ZZVZ*MTY4NzE5NDA2OC4xLjEuMTY4NzE5NDc3My4wLjAuMA..

Kivunja, C., & Kuyini, A. B. (2017). Understanding and Applying Research Paradigms in Educational Contexts. *International Journal of Higher Education*, *6*(5), 26. https://doi.org/10.5430/ijhe.v6n5p26

Klaus Schwab. (2016, January 14). *The Fourth Industrial Revolution: What it means and how to respond*. World Economic Forum. https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/

Kock, N. (2019). *WarpPLS User Manual: Version 6.0*.

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

Liang, X., Konstantinou, C., Shetty, S., Bandara, E., & Sun, R. (2023). Decentralizing Cyber Physical Systems for Resilience: An Innovative Case Study from A Cybersecurity Perspective. *Computers & Security*, *124*, 102953. https://doi.org/10.1016/j.cose.2022.102953

Maalem Lahcen, R. A., Caulkins, B., Mohapatra, R., & Kumar, M. (2020). Review and insight on the behavioral aspects of cybersecurity. *Cybersecurity*, *3*(1), 10. https://doi.org/10.1186/s42400-020-00050-w

Madden, T. J., Ellen, P. S., & Ajzen, I. (1992). A Comparison of the Theory of Planned Behavior and the Theory of Reasoned Action. *Personality and Social Psychology Bulletin*, *18*(1), 3–9. https://doi.org/10.1177/0146167292181001

Mahlobo, M. D. (2015). *National Cybersecurity Policy Framework*.

Maliti, S. (2022, December 15). *FBI beat security cluster in identifying cyber hack of the SA Reserve Bank, says Godongwana*. https://www.iol.co.za/capeargus/news/fbi-beat-security-cluster-in-identifying-cyber-hack-of-the-sa-reserve-bank-says-godongwana-0c5e9af6-00e2-45bd-9867-a386cd351db7

Martilla, J. A., & James, J. C. (1977). Importance-Performance Analysis. *Journal of Marketing*, *41*(1), 77–79. https://doi.org/10.2307/1250495

Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data Privacy: Effects on Customer and Firm Performance. *Journal of Marketing*, *81*(1), 36–58. https://doi.org/10.1509/jm.15.0497

Merton, R. K. (1938). Social Structure and Anomie. *American Sociological Review*, *3*(5), 672–682. https://doi.org/10.2307/2084686

MITRE ATT&CK®. (n.d.). Retrieved May 27, 2024, from https://attack.mitre.org/

Moberly, M. D. (2014). Chapter 1—Intangible Assets. In M. D. Moberly (Ed.), *Safeguarding Intangible Assets* (pp. 1–11). Butterworth-Heinemann. https://doi.org/10.1016/B978-0-12-800516-3.00001-X

Modise, E. (2023, April 19). South Africa is the cybercrime hub of Africa, according to INTERPOL. *TechCabal*. https://techcabal.com/2023/04/19/south-africa-interpol-cybercrime/

Mohammed, D. (2015). *Cybersecurity Compliance in the Financial Sector*. *20*(1).

Moyo, A. (2022, March 17). *BREAKING: Credit bureau TransUnion hacked*. ITWeb. https://www.itweb.co.za/content/o1Jr5Mx9BVjqKdWL

Mukherjee, P. (2020, August 20). South Africa banks offered loan relief of $31 billion during pandemic: Statement. *Reuters*. https://www.reuters.com/article/us-health-coronavirus-safrica-banks-idUSKBN25G2DD

Muncaster, P. (2020, August 20). *Experian Data Breach Hits Estimated 24 Million Customers*. Infosecurity Magazine. https://www.infosecurity-magazine.com/news/experian-data-breach-24-million/

National Cyber Strategy. (2022).

Ndiga, B., Mumiukhacatherine Khakasa, C., Flora, F., Ngugi, M., & Mwalwa, S. (2014). Principals' Transformational Leadership Skills in Public Secondary Schools: A Case of Teachers' and Students' Perceptions and Academic Achievement in Nairobi County, Kenya. *American Journal of Educational Research*, *2*(9), 801–810. https://doi.org/10.12691/education-2-9-15

Novaes Neto, N., Madnick, S. E., Moraes G. De Paula, A., & Malara Borges, N. (2020). A Case Study of the Capital One Data Breach. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3542567

Nunkoo, R., & Ramkissoon, H. (2011). Structural equation modelling and regression analysis in tourism research. *Current Issues in Tourism*, *15*, 1–26. https://doi.org/10.1080/13683500.2011.641947

Palko, D., Babenko, T., Bigdan, A., Kiktev, N., Hutsol, T., Kuboń, M., Hnatiienko, H., Tabor, S., Gorbovy, O., & Borusiewicz, A. (2023). Cyber Security Risk Modeling in Distributed Information Systems. *Applied Sciences*, *13*(4), Article 4. https://doi.org/10.3390/app13042393

Parker, A., & Brown, I. (2019). Skills Requirements for Cyber Security Professionals: A Content Analysis of Job Descriptions in South Africa. In H. Venter, M. Loock, M. Coetzee, M. Eloff, & J. Eloff (Eds.), *Information Security* (pp. 176–192). Springer International Publishing. https://doi.org/10.1007/978-3-030-11407-7_13

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

Poire, B. A. L., & Dailey, R. M. (2006). *Applied Interpersonal Communication Matters: Family, Health, & Community Relations*. Peter Lang.

Ponemon Institute. (2022, July). *Cost of a data breach 2022 | IBM*. https://www.ibm.com/reports/data-breach

Prof. Elton Mayo. (1934). The Human Problems of an Industrial Civilization. *Nature*, *134*(3380), Article 3380. https://doi.org/10.1038/134201b0

Rachida Parks, Heng Xu, Chao-Hsien Chu, & Paul Benjamin Lowry. (2016, May 4). *Examining the intended and unintended consequences of organisational privacy safeguards—ProQuest*. https://www.proquest.com/docview/1867925495/E936006CEBF5488EPQ/1?accountid=15083&sourcetype=Scholarly%20Journals

Ramezan, C. A. (2023). *Examining the Cyber Skills Gap: An Analysis of Cybersecurity Positions by Sub-Field*.

Rebecca Sansom. (2021). *Theory of Planned Behavior*. Change Theories Collection. https://ascnhighered.org/ASCN/change_theories/collection/planned_behavior.html

Roopa, S., & Rani, M. (2012). Questionnaire Designing for a Survey. *Journal of Indian Orthodontic Society*, *46*(4_suppl1), 273–277. https://doi.org/10.5005/jp-journals-10021-1104

Sangmi Chai. (2009, April 28). *Three essays on behavioral aspects of information systems: Issues of information assurance and online privacy - ProQuest*. https://www.proquest.com/docview/305087895/E936006CEBF5488EPQ/3?accountid=15083&sourcetype=Dissertations%20&%20Theses

Sarah Slight, Kathrin Cresswell, Ann Robertson, & Guro Huby. (2011, June). *(PDF) The Case Study Approach*. https://www.researchgate.net/publication/51252479_The_Case_Study_Approach

Sarver, V. T. (1983). Ajzen and Fishbein's "theory of reasoned action": A critical assessment. *Journal for the Theory of Social Behaviour*, *13*(2), 155–163. https://doi.org/10.1111/j.1468-5914.1983.tb00469.x

Seals, G. (2013). *An Ethics Paradigm for the Service Organization*. *2*(3).

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

Shrum, W. (2001). Science and Development. In N. J. Smelser & P. B. Baltes (Eds.), *International Encyclopedia of the Social & Behavioral Sciences* (pp. 13607–13610). Pergamon. https://doi.org/10.1016/B0-08-043076-7/03165-X

Singh, C., Chauhan, D., Deshmukh, S. A., Vishnu, S. S., & Walia, R. (2021). Medi-Block record: Secure data sharing using block chain technology. *Informatics in Medicine Unlocked*, *24*, 100624. https://doi.org/10.1016/j.imu.2021.100624

Stone, M. (1974). Cross-Validatory Choice and Assessment of Statistical Predictions. *Journal of the Royal Statistical Society: Series B (Methodological)*, *36*(2), 111–133. https://doi.org/10.1111/j.2517-6161.1974.tb00994.x

Thomas Sarver Jr., V. (1983). Ajzen and Fishbein's "Theory of Reasoned Action": A Critical Assessment. *Journal for the Theory of Social Behaviour*, *13*(2), 155–164. https://doi.org/10.1111/j.1468-5914.1983.tb00469.x

Tim Stobierski. (2021, February 2). *8 Steps in the Data Life Cycle | HBS Online*. Business Insights Blog. https://online.hbs.edu/blog/post/data-life-cycle

Tobias Adrian & Caio Ferreira. (2023, February 3). *Mounting Cyber Threats Mean Financial Firms Urgently Need Better Safeguards*. IMF. https://www.imf.org/en/Blogs/Articles/2023/03/02/mounting-cyber-threats-mean-financial-firms-urgently-need-better-safeguards

Tsakanikas, A., Caloghirou, Y., Dimas, P., & Stamopoulos, D. (2022). Intangibles, innovation, and sector specialization in global value chains: A case study on the

EU's and the UK's manufacturing industries. *Technological Forecasting and Social Change*, *177*, 121488. https://doi.org/10.1016/j.techfore.2022.121488

Van Heerden, R., Von Soms, S., & Mooi, R. (2016). Classification of cyber attacks in South Africa. *2016 IST-Africa Week Conference*, 1–16. https://doi.org/10.1109/ISTAFRICA.2016.7530663

W. Alec Cram, Jeffrey G. Proudfoot, & John D'Arcy. (2017, June 14). *Organizational information security policies: A review and research framework - ProQuest*. https://www.proquest.com/docview/1966722376/E936006CEBF5488EPQ/2?accountid=15083&sourcetype=Scholarly%20Journals

Wall, J., Lowry, P. B., & Barlow, J. B. (2015). *Organizational Violations of Externally Governed Privacy and Security Rules: Explaining and Predicting Selective Violations Under Conditions of Strain and Excess* (SSRN Scholarly Paper 2611567). https://papers.ssrn.com/abstract=2611567

Walton, S., Wheeler, P. R., Zhang, Y. (Ian), & Zhao, X. (Ray). (2021). An Integrative Review and Analysis of Cybersecurity Research: Current State and Future Directions. *Journal of Information Systems*, *35*(1), 155–186. https://doi.org/10.2308/ISYS-19-033

Yang, G., Yang, M., Salam, S., & Zeng, J. (2019). Research on Protecting Information Security Based on the Method of Hierarchical Classification in the Era of Big Data.

Computers, Materials & Continua, *61*(3), 19–26. https://doi.org/10.32604/jcs.2019.05947

Zimmeck, S., Wang, O., Alicki, K., Wang, J., & Eng, S. (2023). Usability and Enforceability of Global Privacy Control. *Proceedings on Privacy Enhancing Technologies*, *2023*(2), 265–281. https://doi.org/10.56553/popets-2023-0052

Appendix A: Data-Collection Instrument

Cybersecurity Perspectives Survey

This survey aims to investigate the perspectives of cybersecurity professionals and stakeholders regarding the protection of intangible commodities in the context of financial institutions in South Africa. The information gathered from this survey will contribute to a case study on cybersecurity practices and challenges within the financial sector. Your participation in this survey is voluntary, and all responses will be kept anonymous and confidential.

Instructions:

Please read each question carefully and select the most appropriate response. Questions are posed utilising the Likert 5-point scale. There are also open-ended questions where you can provide detailed responses. Your insights and opinions are valuable, and we appreciate your time and effort in completing this survey.

Section 1: Demographic Information

1. Gender:

☐ Male ☐ Prefer not to say

☐ Female ☐ Other (please specify :)

2. Age:

☐ 18-24 ☐ 45-54

☐ 25-34 ☐ 55 or above

☐ 35-44

3. Job Title/Position:

☐ Cybersecurity professional ☐ Compliance officer

☐ IT manager ☐ Executive/Management

☐ Risk manager ☐ Other (please specify:)

4. Years of Experience in Cybersecurity:

☐ Less than 1 year ☐ 7-10 years

☐ 1-3 years ☐ More than 10 years

☐ 4-6 years

Section 2: Cybersecurity Perspectives on Protecting Intangible Commodities

The perceived risk of violating a privacy or cybersecurity rule negatively affects the likelihood of a privacy or security rule violation aimed at safeguarding intangible commodities.

1. How would you rate your perception of the risk associated with violating privacy or cybersecurity rules? (On a scale of 1 to 5)

2. How likely are you to engage in a privacy or security rule violation aimed at protecting intangible commodities? (On a scale of 1 to 5)

3. How concerned are you about the potential consequences of violating privacy or cybersecurity rules? (On a scale of 1 to 5)

4. Do you believe that violating privacy or cybersecurity rules poses significant risks to intangible commodities? (On a scale of 1 to 5)

5. How much does the perceived risk of rule violation influence your decision-making regarding privacy and cybersecurity practices? (On a scale of 1 to 5)

Both formal and informal communication structures that promote regulatory compliance will heighten the perception of risk regarding rule violation for individuals and organisations.

6. To what extent do formal communication structures in your organisation promote regulatory compliance? (On a scale of 1 to 5)

7. To what extent do informal communication channels within your organisation emphasize the importance of adhering to rules and regulations? (On a scale of 1 to 5)

8. How do formal and informal communication structures influence your perception of the risks associated with rule violation? (On a scale of 1 to 5)

9. Are you more aware of the potential risks of rule violation due to effective communication about compliance? (On a scale of 1 to 5)

10. How does the level of communication about compliance affect your perception of the consequences of rule violation? (On a scale of 1 to 5)

Instances of violations linked to negative outcomes will increase the perception of risk associated with rule violation for individuals and organisations.

11. Have you or your organisation experienced any violations of privacy or cybersecurity rules that resulted in negative consequences? (On a scale of 1 to 5)

12. How did witnessing or experiencing such violations affect your perception of the risks associated with rule violation? (On a scale of 1 to 5)

13. How likely are you to perceive rule violation as risky after learning about the negative outcomes of others who violated the rules? (On a scale of 1 to 5)

14. How do instances of rule violations affecting others influence your own perception of the risks associated with rule violation? (On a scale of 1 to 5)

15. Does knowledge of past violations make you more cautious about the consequences of potential rule violation? (On a scale of 1 to 5)

The enforceability of regulations will positively impact the perception of risk of rule violation for individuals and organisations.

16. Do you believe that the regulations related to privacy and cybersecurity are effectively enforced in your organisation or community? (On a scale of 1 to 5)

17. How does the level of enforcement influence your perception of the risks associated with rule violation? (On a scale of 1 to 5)

18. Are you more likely to perceive rule violation as risky when you believe that regulations are enforced consistently? (On a scale of 1 to 5)

19. Does the perception of strong enforcement make you more cautious about potential rule violation? (On a scale of 1 to 5)

20. How do past experiences with rule enforcement influence your perception of the risks of future rule violation? (On a scale of 1 to 5)

The clarity of goals in rules and regulations will positively influence the perception of risk of violating those rules for individuals and organisations.

21. To what extent do you find the rules and regulations related to privacy and cybersecurity clear and easy to understand? (On a scale of 1 to 5)

22. How does the clarity of goals in these rules affect your perception of the risks associated with rule violation? (On a scale of 1 to 5)

23. Are you more likely to perceive rule violation as risky when the goals of the rules are clearly defined? (On a scale of 1 to 5)

24. Does a lack of clarity in rules make you more hesitant about potential rule violation? (On a scale of 1 to 5)

25. How do you interpret the risks associated with rule violation when the goals of the rules are ambiguous? (On a scale of 1 to 5)

Connectedness (presumably referring to network connections or relationships) will positively influence the perception of risk of violating rules for individuals and organisations.

26. How interconnected do you feel within your organisation or community regarding compliance with privacy and cybersecurity rules? (On a scale of 1 to 5)

27. How does your level of connectedness impact your perception of the risks associated with rule violation? (On a scale of 1 to 5)

28. Are you more likely to perceive rule violation as risky when you have strong connections with others who value compliance? (On a scale of 1 to 5)

29. Does the support from your network influence your attitude towards the risks of rule violation? (On a scale of 1 to 5)

30. How do interactions with others who comply with rules affect your perception of the risks of violating those rules? (On a scale of 1 to 5)

A positive attitude towards rule-abiding behaviour will positively influence the perception of risk of violating rules for individuals and organisations.

31. How would you describe your attitude towards adhering to privacy and cybersecurity rules? (On a scale of 1 to 5)

32. How does your attitude towards rule-abiding behaviour affect your perception of the risks associated with rule violation? (On a scale of 1 to 5)

33. Are you more cautious about rule violation when you believe in the importance of compliance? (On a scale of 1 to 5)

34. Does a positive attitude towards rules and regulations affect your decision-making regarding potential violations? (On a scale of 1 to 5)

35. How do your beliefs about the benefits of compliance influence your perception of the risks of rule violation? (On a scale of 1 to 5)

Subjective norms will positively influence the perception of risk of violating rules for individuals.

36. How much do you feel social pressure from others to comply with privacy and cybersecurity rules? (On a scale of 1 to 5)

37. How do subjective norms influence your perception of the risks associated with rule violation? (On a scale of 1 to 5)

38. Are you more likely to perceive rule violation as risky when others around you emphasize the importance of compliance? (On a scale of 1 to 5)

39. Does the influence of subjective norms impact your decision-making regarding potential rule violations? (On a scale of 1 to 5)

40. How do your perceptions of social expectations influence your perception of the risks of rule violation? (On a scale of 1 to 5)

Section 3: Additional Comments

12. Please provide any additional comments or insights regarding the protection of intangible commodities in financial institutions in South Africa.

Thank you for participating in this survey. Your responses will contribute to valuable insights and findings in the field of cybersecurity and its impact on protecting intangible commodities in financial institutions in South Africa.

Appendix B: Survey Participation Request



Dear Participant.

My name is Trevor Naidoo. I am a Masters student pursuing a Master's of Management degree in Digital Business at the Wits Business School. I am conducting a research study about the protection of intangible commodities within the South African financial services supervised by Prof. Nixon Ochara.

The study title is: “Cybersecurity Perspectives on Protecting Intangible Commodities in the South African Financial Sector”

I am inviting you to participate in the study by completing an online survey. The online survey can be done at your convenience and will take approximately 15 minutes to complete.

The survey is confidential and anonymous. Your participation is voluntary, and you are free to withdraw at any time.

The information you provide will be kept confidential, and no identifiable information will be used in the dissemination of the results. By taking part in the survey, you are acknowledging your consent to take part in the study.

This research study will be written up as a research report. The report will be available on the university library website. If you would like to receive a summary of this report, I will be happy to send it to you.

If you have any questions during or afterwards about this research study, feel free to contact me or my supervisor on the details listed below. If you have any concerns or complaints about the ethical procedures of this research study, you are welcome to contact the University Human Research Ethics Committee (Non-Medical), telephone +27(0) 11 717 1408, email hrecnon-medical@wits.ac.za.

Yours sincerely,

Trevor Naidoo

Researcher:

Trevor Naidoo, 851470@students.wits.ac.za, +27 71 495 7620

Supervisor:

Prof. Nixon Ochara, nixon.ochara@wits.ac.za , +27 72 170 4560

Appendix C: Ethics Clearance Certificate

Graduate School of Business Administration
University of the Witwatersrand, Johannesburg

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

Ethics Clearance Certificate

Ethics protocol number: WBS/DB851470/819

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

Project title	Cybersecurity perspectives on protecting intangible commodities in the South African financial sector
Investigator / Researcher	Mr Trevor Naidoo
Nature of Project	MM (Digital Business)
Decision of the Committee	Approved, provided stakeholders and participants are guaranteed anonymity and confidentiality.
Issue Date of Certificate	2023/10/15
Expiry date	Date of submission of the project / research report
Chairperson	Dr Pius Oba ☎ +27 11 717 3976 +27 82 733 6587 pius.oba@wits.ac.za

Declaration by Researcher

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

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

Trevor Naidoo
Signature

16 October 2023
Date: