https://dspace.org/

Exploring Technical Implementation of Cybersecurity Measures within Small and Medium Enterprises (SMEs) in the South African Market

Baloyi, Dineo

2025

University of the Witwatersrand, Johannesburg

https://hdl.handle.net/10539/47849

Baloyi, Dineo . (2025). Exploring Technical Implementation of Cybersecurity Measures within Small and Medium Enterprises (SMEs) in the South African Market [Master`s dissertation, University of the Witwatersrand, Johannesburg]. WIReDSpace. https://hdl.handle.net/10539/47849

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

Exploring Technical Implementation of Cybersecurity Measures within Small and Medium Enterprises (SMEs) in the South African Market

Dineo Baloyi

0714395M

Supervisor: Dr Zubeida Dawood

A research report 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

Small and Medium Enterprises (SMEs) are integral to South Africa's economy, contributing up to 40% of GDP. However, they remain highly vulnerable to evolving cyber threats due to resource constraints, limited expertise, and challenges in regulatory compliance. This study explores the technical implementation, effectiveness, and challenges of cybersecurity measures in South African SMEs across four key sectors, namely financial services, retail and e-commerce, manufacturing, and mining.

Using an interpretivist, qualitative research approach, the study gathered insights from semi-structured interviews with thirteen SMEs and document analysis to uncover cybersecurity practices and challenges.

The research integrates the Resource-Based View (RBV), Diffusion of Innovations (DOI), and Technology Acceptance Model (TAM) to contextualise adoption behaviours and internal capabilities.

Findings show limited adoption of advanced security measures due to cost, lack of expertise, and the complexity of POPIA compliance. Practical recommendations include cost-effective AI-driven solutions, improved cybersecurity literacy, and sector-specific policy support.

This research contributes contextually by highlighting sectoral differences, methodologically by combining interview and document analysis, and theoretically by applying and extending RBV, DOI, and TAM frameworks in an emerging market context.

KEYWORDS

Cybersecurity, SMEs, South Africa, Regulatory Compliance, Digital Resilience

DECLARATION

I, Dineo Baloyi, declare that this research report is my own work except as indicated in the references and acknowledgements. It is submitted in partial fulfilment of the requirements for the degree of Master of 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: Dineo Baloyi Signature:

Signed at Midrand

On the 24 day of February 2025

DEDICATION

I dedicate my research paper to my parents, whose efforts and steadfast love have moulded me into the person I am today. Even though you are no longer with me, I always find strength in your ideals and wisdom. To my beloved mother, who passed February 2024 while I had already begun this journey, your memories motivated me to keep going even at the most trying times of grief and adversity. I hope that this accomplishment honours the legacy that you both left. This work is also dedicated to my amazing husband, who supported me during this trying time. I was able to get through times when the weight of this trip felt too much to carry because of your constant encouragement, patience, and support. I appreciate your support and belief in me during the entire process.

ACKNOWLEDGEMENTS

First and foremost, I want to express my sincere gratitude to Dr. Zubeida Dawood, my supervisor, for her tremendous advice, insight, and support along this journey. I was inspired to do my best work and approach my task with more depth and insight by your knowledge and steadfast support.

To my children, I am aware that my studies prevented me from spending many weekends and moments with you, but your tolerance and smiles have been my biggest source of inspiration.

I want to thank my employer from the bottom of my heart for supporting my education and giving me the chance to take a study leave whenever required. This accomplishment was made possible by your faith in my abilities and commitment to my development. I would want to express my gratitude to my line manager for his understanding and assistance during this time, particularly when I needed flexibility to manage my studies and work.

To my entire family, thank you for standing by me throughout this challenging journey. Your encouragement, support, and love provided the foundation I needed to persevere during difficult moments.

Finally, to my friends and classmates, thank you for your camaraderie, shared laughs, and words of encouragement. This journey was made richer and more enjoyable because of you all.

TABLE OF CONTENTS

ABSTRACT ..... **ii**

KEYWORDS ..... **iii**

DECLARATION ..... **iv**

DEDICATION ..... **v**

ACKNOWLEDGEMENTS ..... **vi**

LIST OF ACRONYMS ..... **xi**

CHAPTER 1. INTRODUCTION **1**

1.1 STATEMENT OF PURPOSE 1
1.2 BACKGROUND OF THE STUDY 1
1.3 RESEARCH PROBLEM 3
1.4 RESEARCH OBJECTIVES 5
1.5 RATIONALE 6
1.6 SCOPE AND INDUSTRY FOCUS 8
1.7 DELIMITATIONS OF THE STUDY 10
1.8 DEFINITION OF TERMS 11
1.9 ASSUMPTIONS 12
1.10 CHAPTER OUTLINE 14

CHAPTER 2. LITERATURE REVIEW AND THEORETICAL FRAMEWORK 16

2.1 INTRODUCTION 16
2.2 DEFINITION OF TOPIC OR BACKGROUND DISCUSSION 16
2.3 GLOBAL LANDSCAPE OF SME CYBERSECURITY THREATS 17
2.4 LOCAL LANDSCAPE OF SME CYBERSECURITY THREATS 19

2.5 Sectors of Focus 22
2.6 Common Cyber Attacks reported 23
2.7 Technical Cybersecurity Measures 25
2.8 Challenges Faced by SMEs in Implementing Cybersecurity Measures 28
2.9 Existing best practices for Cybersecurity Solutions within SMEs 30
2.10 Key Themes from the literature 31
2.11 Analytical Framework 32
Theoretical Framework 32
2.12 Conclusion of Literature Review 34

CHAPTER 3. RESEARCH METHODOLOGY 37

3.1 Research Paradigm 37
3.2 Research approach 38
3.3 Research Design and Justification 39
3.4 Data collection methods 39
3.5 Population and sample 40
3.5.1 Population 40
3.5.2 Sample and sampling method. 40
3.6 The research instrument 43
3.7 Procedure for data collection 44
3.8 Data analysis strategies and interpretation 45
3.9 Possible limitations and challenges of the study 48
3.10 Self-Reflexivity 48
3.11 Quality Assurance 49
3.11.1 External validity OR transferability 49
3.11.2 Internal validity OR credibility 50
3.11.3 Reliability OR dependability 50
3.12 Ethical considerations 50

CHAPTER 4. FINDINGS AND ANALYSIS 54

4.1 Introduction 54
4.2 Background for Participants and Companies 55
4.2.1 Overview of Participants 55
4.2.2 An Overview of Companies Involved. 58
4.2.3 Geographic Representation of Participating Companies 61
4.3 Thematic Analysis 62
4.3.1 Step 1: Codes 63
4.3.2 Step 2 Develop the Themes 64

4.4 Cybersecurity Documentation and Logs 70
4.5 Participant Quotes and Insights 71
4.6 Summary of Findings 73

CHAPTER 5. DISCUSSION OF THE FINDINGS 75

5.1 Introduction 75
5.2 Discussion of Findings in Relation to Literature 75
5.2.1 The Impact of Financial Constraints on Cybersecurity 77
5.2.2 The Role of Expertise in Cybersecurity Implementation 78
5.2.3 Regulatory Pressures and Compliance Challenges 79
5.2.4 The Role of Proactive Resilience 81
5.3 Implications for SMEs and Cybersecurity Practices 82
5.4 Linking Cybersecurity Measures to Industry Standards 84
5.5 Addressing the Research Objectives 85
5.6 Comparative Analysis of Interview and Literature Findings 87
5.7 Narrative Analysis of Cybersecurity Maturity 89
5.7.1 Pattern Analysis 89
5.7.2 Insights 90
5.8 Theoretical Reflections 91
5.8.1 Alignment with Theoretical Expectations 91
5.8.2 Divergence from Theoretical Expectations 92
By considering these behavioural factors, we can better understand why some SMEs fail to invest in cybersecurity, even when they acknowledge the risks of inaction. 93
5.9 Chapter Conclusion 93

CHAPTER 6. CONCLUSIONS & RECOMMENDATIONS 98

6.1 Introduction 98
6.2 Contributions 99
6.3 Summary of Key Findings 100
6.4 Recommendations 100
6.4.1 For SMEs 100
6.4.2 Recommendations For Policymakers 105
6.4.3 Practical Implications for SME Owners 106
6.4.4 Simplify Regulatory Requirements for SMEs 106
6.5 Limitations of the Study 107
6.6 Amended Framework 108
6.7 Suggestions for Future Research 109
6.8 Conclusion 110

REFERENCES 113

APPENDIX (A) Instrument 119

APPENDIX (B) Consent Form..... 122

APPENDIX (C) Participation Information Sheet 123

APPENDIX (D) Ethics Approval Letter..... 125

LIST OF ACRONYMS

AES - Advanced Encryption Standard

AI - Artificial Intelligence

CIPC - Companies and Intellectual Property Commission

CDAS - Cybersecurity Data Analytics System

CIS - Centre for Internet Security

CSA - Cybersecurity Awareness

DJ&CD - Department of Justice and Constitutional Development

DOI - Diffusion of Innovations (Theory)

FSCA - Financial Sector Conduct Authority

GDP – Gross Domestic Product

GDPR - General Data Protection Regulation

HIDS - Host Intrusion Detection System

ICS - Industrial Control Systems

ICT - Information and Communication Technology

IEC - International Electrotechnical Commission

IDS - Intrusion Detection System

ISNCC - International Symposium on Networks, Computers and Communications

ISO - International Organization for Standardization

ITWEB - IT Web (Publication)

KCA - Kenya College of Accountancy

MFA - Multifactor Authentication

MSP - Managed Service Provider

NIDS - Network-based Intrusion Detection System

NIST - National Institute of Standards and Technology

OT - Operational Technology

POPIA - Protection of Personal Information Act

PWC - PricewaterhouseCoopers

RBV - Resource-Based View

ROI - Return on Investment

SARB - South African Reserve Bank

SEDA - Small Enterprise Development Agency

SIEM - Security Information and Event Management

SMME - Small, Medium, and Micro Enterprises

SME – Small and Medium Enterprises

SSL - Secure Sockets Layer

TAM - Technology Acceptance Model

TLS - Transport Layer Security

UJ-TRCTI - University of Johannesburg Technology Research Centre for Innovation (UJ-TRCTI)

CHAPTER 1. INTRODUCTION

1.1 Statement of purpose

This study aimed to explore the technical deployment, effectiveness, and challenges of cybersecurity solutions within Small and Medium Enterprises (SMEs) in the South African market, with the goal of providing insights to enhance technical defences and protect SMEs digital assets and operations against cyber threats.

This research further aimed to contribute to the academic understanding of SME cybersecurity in emerging markets through the application of Resource-Based View (RBV), Diffusion of Innovations (DOI), and Technology Acceptance Model (TAM) theories. It also offered a contextual perspective relevant to regulatory environments like Protection of Personal Information Act (POPIA), thereby informing both scholarly literature and policy development.

1.2 Background of the study

The increasing frequency and complexity of cyber threats present a significant risk to Small and Medium Enterprises (SMEs) worldwide, with recent statistics indicating a troubling surge in cyber-attacks targeting businesses of all sizes(World Economic Forum, 2024). The World Economic Forum reports that in the first half of 2023 alone, ransomware attack instances rose by 50% year over year, highlighting the critical need for strong cybersecurity measures across industries(World Economic Forum, 2024). SMEs in South Africa should be especially concerned about these vulnerabilities.

According to the World Bank, SMEs make up a significant amount of South Africa's economy and can account for as much as 40% of its GDP (World Bank, 2019). Despite their economic significance, SMEs often struggle to implement

and maintain effective cybersecurity measures, leaving them vulnerable to cyber threats that can disrupt business continuity and compromise the security of sensitive data.

Even though cybersecurity issues are a global concern, this study's South African setting provided special insights into the particular dynamics and difficulties that SMEs in the country faces. Notably, SMEs frequently encounter severe financial and human resource limitations that make it difficult for them to put strong cybersecurity safeguards in place. Furthermore, a large number of SMEs in South Africa are more susceptible to cyberattacks since they lack proper knowledge and training on cybersecurity dangers and best practices (Alexander, 2021). The socioeconomic environment of South Africa offers a complex viewpoint on cybersecurity implementation since it is made up of both urban and rural SMEs working in a variety of industries (UJ-TRCTI, 2022). The cybersecurity preparedness of SMEs in South Africa is greatly impacted by the digital divide. While rural SMEs frequently face limited connectivity, outdated technology, and insufficient digital literacy, urban-based SMEs tend to have better access to high-speed internet, advanced IT infrastructure, and cybersecurity expertise (Mbatha, 2024). This disparity makes it more difficult for rural SMEs to adopt critical security measures. A study examining the digital divide as a barrier to technology adoption by small, medium, and micro enterprises (SMMEs) in the agribusiness sector in Tshwane, South Africa, found that high costs, limited funds, and lack of technical know-how are significant obstacles to ICT adoption(Mbatha, 2024).

Regulatory challenges further complicate cybersecurity implementation for SMEs. Compliance with legislation such as the Protection of Personal Information Act (POPIA) is resource-intensive, posing difficulties for financially constrained SMEs(Botha et al., 2015). Research indicates that many SMEs lack awareness and capacity regarding their legal obligations under POPIA, leading to inconsistent adoption of security practices(Botha et al., 2015).

These socio-economic realities often force SMEs to adopt reactive rather than proactive security strategies. Assessing how these challenges impact SMEs

ability to implement and maintain effective cybersecurity measures is crucial for developing tailored solutions to enhance cybersecurity resilience across different sectors.

The contextual factors shaping cybersecurity practices in South Africa, such as economic disparities, regulatory environments, and technological infrastructure, offer critical insights for people who make policies, industry stakeholders, and SME owners in other regions facing similar challenges. Furthermore, the findings of this study in South Africa hold relevance for similar contexts globally, particularly in emerging economies facing comparable challenges in the technical implementation of cybersecurity measures for SMEs (Kabanda et al., 2018)

The study aimed to understanding these technical challenges and proposing viable solutions to ensure that SMEs continue to contribute effectively to South Africa's GDP while safeguarding their digital assets against evolving cyber threats and regulatory requirements.

1.3 Research Problem

The sharp rise in cyberattacks necessitated an investigation and comprehension of the technological application of cybersecurity measures in South African SMEs. A study by Chingworo aimed to investigate the current cybersecurity practices of these enterprises, assess their effectiveness in mitigating cyber threats, identify challenges in adopting and maintaining these measures, and propose strategies to enhance the technical cybersecurity defense of SMEs (Chingoriwo, 2022). Cyber-attacks have become more sophisticated and frequent, posing significant risks to the confidentiality, integrity, and availability of critical personal and business data (Eybers & Mvundla, 2021). Despite the

increasing threat landscape, many SMEs lack the necessary resources and expertise to implement robust cybersecurity measures, making them vulnerable to cyber-attacks(Alahmari & Duncan, 2021).

The rise in reported cyber-attacks globally is increasing at an average yearly rate of 21% between 2014 and 2023, according to the World Bank report by

(Cobos, 2024), which highlights the evolving threat picture. Developing nations are particularly at risk due to their fast digitisation and weak cybersecurity efforts. This study places itself within this global context, focusing on the cybersecurity preparedness of South African SMEs, which are critical to the country's economy. Therefore, understanding the barriers and opportunities for improving cybersecurity in SMEs is crucial for enhancing their resilience and protecting their digital assets.

Recent incidents underscore the urgency of addressing cybersecurity in South African SMEs. For instance:

- A ransomware attack on the Department of Justice and Constitutional Development (DJ&CD) in 2021 rendered its systems inoperable and revealed weaknesses in the government. Significant financial fines and service interruptions resulted from this attack (Moyo, 2024b).
- Another attack on the DJ&CD in May 2024 disrupted child maintenance payments and exposed ongoing cybersecurity flaws (Moyo, 2024b).
- In March 2024, the Companies and Intellectual Property Commission (CIPC) experienced a breach that exposed the dangers of insufficient security measures for vital systems, impacting the private information of more than three million organisations (Costa, 2024)
- A global IT failure involving Crowdstrike in July 2024 had a significant impact on Capitec Bank, causing banking services to be disrupted and increasing worries regarding reliance on third-party systems (Moyo, 2024a).

- In September 2024, a statement by Fortinet revealed that there was a breach(Fortinet, 2024). Which demonstrates that even organisations with advanced security measures in place are not immune to cyber incidents. For SMEs with fewer resources and less technical expertise, the potential impact of similar breaches is even more severe.
- Most recently, in January 2025, telecommunication company Cell C reported a breach where unauthorised parties accessed sensitive customer data. This incident demonstrates the private sector's vulnerability and underscores the financial and reputational damages associated with such breaches (Malinga, 2025).
- The digital trust insights survey 2025 report by PWC revealed that South African organisations face substantial financial impacts from data breaches, ranging from R1.7 million to over R8.7 million per incident(PWC, 2024). Furthermore, 66% of South African large businesses prioritise mitigating cyber risks, indicating a growing awareness but limited capacity to address threats effectively(PWC, 2024). Despite these efforts, challenges such as inadequate investment, technical expertise, and regulatory compliance continue to impede progress.

These incidents and insights emphasise the critical need to strengthen the cybersecurity posture of South African SMEs. By investigating the current state of technical measures, this study sought to contribute to the broader understanding of cybersecurity challenges and opportunities, offering actionable recommendations for building resilience in the SME sector

1.4 Research Objectives

The main aim of this research was to address the critical issue of cybersecurity implementation within Small and Medium Enterprises (SMEs) in the South African market. Given the rapid increase in cyber-attacks and the evolving nature of cyber threats, it was important to understand how SMEs were managing their cybersecurity infrastructure, the effectiveness of these measures, the challenges

they faced, and the potential strategies they could adopt to enhance their cybersecurity. The research objectives were designed to investigate these aspects and provide actionable insights for SMEs to better protect their digital assets and operations.

1. Evaluate the current technical cybersecurity measures deployed within Small and Medium Enterprises (SMEs) in the South African market and evaluate their effectiveness in mitigating cyber threats.
2. Identify the challenges faced by SMEs in implementing and maintaining technical cybersecurity measures.
3. Investigate potential strategies and best practices to optimise the deployment and utilisation of technical cybersecurity measures within SMEs.

1.5 Rationale

Professional experience as a solution architect for an ICT company, where the job involves designing solutions for businesses including cloud, networking, cybersecurity, IoT, and more, sparked interest in this issue. This position exposes one to the intricacies and difficulties that large corporations encounter. The challenges that resource-rich businesses encounter have sparked curiosity about the even more significant cybersecurity issues that smaller businesses probably face. The obstacles for SMEs are anticipated to be even greater if large corporations, which possess enormous resources, struggle to establish effective cybersecurity. Gaining insight into the cybersecurity experiences of large businesses contextualises the unique needs of SMEs in South Africa, where limited resources heighten the impact of cyber threats.

Large businesses, with their extensive resources and sophisticated infrastructure, encounter several hurdles that highlight the broader landscape of

cybersecurity and technological integration(Ncubukezi, 2023). Examples of such complexities include adapting to intelligent threat , implementing advanced security technologies, balancing financial constraints and security needs and many more(Alexander, 2021). These complexities faced by large businesses underscore the importance of tailored cybersecurity strategies for SMEs. Understanding these challenges provided a rationale for focusing on the unique needs of SMEs in the South African market, where resources are limited, and the impact of cyber threats can be particularly devastating. Understanding these larger-scale challenges highlights the necessity of designing cost-efficient yet robust cybersecurity measures to protect SMEs assets and continuity without the same level of resources available to larger companies.

The empirical rationale for this study is grounded in the increasing frequency and sophistication of cyber threats targeting SMEs (World Economic Forum, 2024), which constitute a significant portion of South Africa's economy. Despite their vital economic role, many SMEs has challenges in implement robust cybersecurity measures, making them vulnerable to cyber-attacks. By investigating the current state of technical cybersecurity measures within South African SMEs, evaluating their effectiveness, and identifying the specific challenges these enterprises encounter, this study aimed to fill a critical gap in the existing literature.

The research was worth conducting because it addresses a pressing need for improved cybersecurity practices among SMEs, which are crucial for maintaining business continuity and protecting sensitive data. The findings from this study provides valuable insights for service providers, policymakers, industry stakeholders, and SME owners, emphasising the importance of prioritising technical cybersecurity measures. Additionally, the study offered actionable recommendations for enhancing the cybersecurity posture of SMEs, thereby contributing to the broader practice of management and digital business.

By translating the empirical findings into practical strategies, this research aimed to add significant value to the practice-oriented utility of cybersecurity in SMEs. It

will support SMEs in implementing more effective technical defences, ultimately fostering a more secure digital business environment in South Africa.

1.6 Scope and Industry Focus

1.6.1. Criteria for Industry Selection

The selection of industries for this study was based on several key criteria

- **Relevance to Service Providers**

  The chosen industries aligned with the strategic interests and service capabilities of cybersecurity providers, ensuring that the findings of this research will have practical applications for their current and potential clients.

- **Cybersecurity Needs**

  The industries selected are known for their high cybersecurity needs due to the sensitive nature of the data they handle and the frequency of cyber-attacks they face.

- **Economic Impact**

  The industries chosen are vital to the South African economy, meaning that improvements in their cybersecurity posture will have significant broader economic benefits.

1.6.2. Selected Industries

Financial Services

Financial institutions are mostly targeted for cyber-attacks due to the high value of financial data. This sector requires robust cybersecurity measures

to protect against threats such as phishing, malware, and ransomware. Cybersecurity solutions can provide critical support in safeguarding financial transactions and customer data.

- **Retail and e-commerce**

With the rapid expansion of e-commerce in South Africa, the retail sector is increasingly exposed to cyber threats such as data breaches and payment fraud. Findings in this study highlight the current cybersecurity measures within SMEs in this sector, revealing both strengths and gaps. Protecting online retail platforms through enhanced cybersecurity practices is critical to safeguarding customer data and maintaining trust in digital transactions, a necessity for sustaining growth and competitiveness in this rapidly evolving industry.

Manufacturing

As manufacturing processes become increasingly digitised, the risk of cyber-attacks targeting both operational technology (OT) and information technology (IT) systems continues to grow. This study examined the cybersecurity practices within SMEs in the manufacturing sector, highlighting vulnerabilities and areas for improvement. Protecting manufacturing systems from cyber threats is vital to preventing production disruptions and financial losses, underscoring the importance of implementing robust cybersecurity measures to secure these critical infrastructures.

Mining

The mining industry, increasingly reliant on digital technologies and automation, is vulnerable to cyber threats that can disrupt operations and compromise safety. Cyber-attacks on mining companies can lead to operational downtime, safety incidents, and financial losses. This research explored the implementation of cybersecurity measures to protect mining

operations, ensuring the integrity of data and the continuous, safe functioning of mining activities.

1.7 Delimitations of the study

I. Focused exclusively on Small and Medium Enterprises (SMEs) operating within the South African market, specifically Financial Services, Retail and E-commerce, Manufacturing and Mining.

II. Excluded larger enterprises and multinational corporations from study scope.

III. Restricted the analysis to South African SMEs, omitting those outside of South Africa, as well as informal or micro businesses in South Africa.

IV. Investigated technical cybersecurity measures specifically related to technology infrastructure.

V. Excluded the analysis of human factors in cybersecurity, as the study solely on technical aspects.

VI. Did not examine broader aspects of cybersecurity governance.

VII. Excluded an in-depth exploration of regulatory compliance issues and broader cybersecurity governance frameworks.

VIII. Did not investigate cybersecurity threats and trends outside the context of SMEs within the South African market.

1.8 Definition of terms

1. **SME –** Small and Medium Enterprises (SMEs) in South Africa are defined according to the National Small Business Act of South Africa, which classifies businesses based on the number of employees and annual turnover(SEDA, 2023). SMEs are categorised into micro, small, small, and medium-sized enterprises. This classification considers factors such as the sector in which the business operates and the maximum turnover thresholds. SMEs play a crucial role in the South African economy, contributing significantly to job creation and economic growth. Despite challenges, including high input costs and inflation, SMEs remain vital for economic development and employment in both the formal and informal sectors(SEDA, 2023)
2. **Cybersecurity –** Cybersecurity refers to the practice of protecting systems, networks, and programs from digital attacks(Kaur et al., 2023). These attacks are usually aimed at accessing, changing, or destroying sensitive information, extorting money from users, or interrupting normal business processes(Naude et al., 2023). In the context of SMEs, effective cybersecurity measures are critical to safeguard digital assets and maintain business continuity.
3. **Technical Cybersecurity Measures –** These are specific technologies and practices implemented to protect the integrity, confidentiality, and availability of information systems and data(Erdogan et al., 2023). Examples include firewalls, encryption, intrusion detection systems, and multifactor authentication. For SMEs, implementing technical cybersecurity measures is essential to defend against cyber threats and comply with regulatory requirements.
4. The term **"technical"** in technical cybersecurity measures refers to the use of specialised tools, technologies, and automated processes to

safeguard information systems from cyber threats(Lindemulder & Kosinski, 2024). Other cybersecurity measures may focus more on policies, training, and compliance but technical measures involve the direct application of hardware and software solutions to detect, prevent, and respond to security incidents(Lindemulder & Kosinski, 2024).

5. **Digital Asset –** encompass any content or media formatted into a binary source and include the right to use it(Rawindaran et al., 2021). These assets include, but are not limited to, digital documents, audio and video files, and digital currencies. For SMEs, digital assets are vital components of their business operations, often containing valuable proprietary information that requires robust protection against unauthorised access and cyber threats.

1.9 Assumptions

In this study, several assumptions were made, each of which influenced the research outcome.

1. **Similarity of Cybersecurity Challenges**

   This study recognised the prevalence of similar cybersecurity challenges faced by SMEs globally, such as phishing attacks, malware infections, and ransomware threats. These challenges stem from the reliance on technology and interconnectedness common to most SMEs worldwide. However, it also acknowledges that the unique socio-economic and regulatory environment in South Africa may introduce distinct challenges for SMEs in this region. While the assumption that South African SMEs face challenges comparable to those in other regions is reasonable, given the global nature of cybersecurity threats, any significant differences in these challenges could limit the study's broader applicability. Nonetheless, recognising and addressing these unique local challenges can enhance relevance and specificity of the study.

2. **Honesty and Transparency**

   It was assumed that SMEs would actively participate in the research and provide accurate, detailed information about their cybersecurity practices and challenges. The validity of the research outcomes is highly dependent on this assumption. If SMEs were unwilling to share information or provided incomplete or inaccurate responses, it could compromise the reliability and robustness of the findings.

3. **Applicability and Beneficial Outcomes**

   The research assumed that the findings and recommendations would be relevant and beneficial for South African SMEs aiming to enhance their cybersecurity resilience. The applicability of the outcomes relied on the thoroughness of the research and its alignment with the practical needs of SMEs. If the findings are not viewed as applicable or beneficial, the impact of the research could be limited. Emphasising practical and context-aware recommendations was critical to mitigating this risk.

4. **Cybersecurity Knowledge and Practices**

   The study assumed that SMEs understood and used cybersecurity measures, even basic. If many SMEs lacked even basic cybersecurity measures, the focus of the study could have shifted towards identifying fundamental gaps in awareness and education.

5. **Benefit from Best Practices**

   The study assumed SMEs can benefit from identified best practices and strategies for optimising the deployment and utilisation of technical cybersecurity solutions. The research outcome is moderately sensitive to this assumption. If SMEs are unable or unwilling to adopt these best practices due to resource constraints or other barriers, the practical impact of the research could be limited.

6. **Assume some Level of literacy and level of digital literacy exist.**

   The study assumed that SMEs in South Africa possess a basic level of general literacy and digital literacy among their employees. This assumption is critical as it underpins the ability of SMEs to understand, implement, and maintain technical cybersecurity measures. The research outcome is highly sensitive to this assumption. If SMEs lack the necessary literacy or digital literacy skills, the effectiveness of proposed cybersecurity solutions and best practices could be significantly diminished.

1.10 Chapter outline

- Chapter 1 introduces and contextualises the research problem, outlining the background and rationale behind the study. This chapter also presents the research questions guiding the investigation in subsequent chapters.

- Chapter 2 provides a review of relevant academic literature on technical cybersecurity measures and challenges faced by SMEs. This chapter examines key theories and research findings in the field, presenting the propositions that address the research questions. The analytical framework that underpins this study is also detailed here.

- Chapter 3 outlines the research methodology employed to collect and analyse data, detailing the study design, data collection methods, sampling approach, and analytical strategies.

- Chapter 4 presents the findings from the data collected, systematically summarising the observed themes and insights related to the research questions.

- Chapter 5 discusses and interprets the findings from Chapter 4, linking them back to the research questions and literature review to provide a comprehensive analysis.

- Chapter 6 concludes the study, summarising key insights and offering recommendations for future research in the field.

In analysing the research findings, the study drew on five key propositions developed in the literature review and grounded in the RBV, DOI, and TAM theoretical frameworks. These propositions provided a structured lens through which the behaviours, practices, and challenges of SMEs are interpreted in the discussion chapter.

CHAPTER 2. LITERATURE REVIEW AND THEORETICAL FRAMEWORK

2.1 Introduction

The literature review served as a critical analysis of existing scholarly work relevant to the implementation of technical cybersecurity measures within Small and Medium Enterprises (SMEs) in the South African market. This section provides an in-depth examination of primary sources, key authors, major debates, fundamental concepts, and prevailing theories related to the research objectives. The aim was to establish a comprehensive understanding of the current state of knowledge and to identify gaps that this study sought to address.

The literature review is structured as follows. First a definition is given, followed by sections on the global and local landscape of SME cybersecurity threats respectively. This is followed by a section by technical cybersecurity measures. Then challenges faced by SMEs in implementing cybersecurity measures according to literature, and before conclusion on literature review, a section on analytical framework.

2.2 Definition of Topic or Background Discussion

The definition and understanding of technical cybersecurity measures within SMEs were crucial to frame this study. Cybersecurity measures refer to the technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorised access (Varachia, 2022). In the context of SMEs, these technical measures often include firewalls, intrusion detection systems (IDS), encryption protocols, and endpoint security software. Given the dynamic nature of cybersecurity threats, SMEs must continuously adapt and upgrade their defense(Alahmari & Duncan, 2021). The

growing reliance on digital technologies has further highlighted the need for robust cybersecurity measures to ensure business continuity and protect sensitive information(Rawindaran et al., 2023).

2.3 Global Landscape of SME Cybersecurity Threats

SMEs around the world face an increasing number of cybersecurity threats that continue to evolve in complexity and frequency(Erdogan et al., 2023). SMEs are now more vulnerable to cyberattacks due to their growing reliance on digital technologies and networked systems (Alahmari & Duncan, 2021). This section explored the various cybersecurity threats faced by SMEs globally, highlighting the trends, types of attacks, and the overall impact on businesses.

The global cybersecurity landscape for Small and Medium Enterprises (SMEs) is characterised by an increasing number of cyber threats and sophisticated attack methods(Department for Science, 2024). SMEs are particularly vulnerable due to limited resources, lack of cybersecurity expertise, and inadequate defensive measures(Kariuki et al., 2023). According to a PwC report, there has been a significant rise in cyberattacks targeting the manufacturing and mining sectors, with 74% of businesses reliant on operational technology frequently encounter major IT security breaches in the preceding 12 months (PWC, 2021). These incidents not only compromise critical data but also result in substantial financial losses and damage to brand reputation.

In Costa Rica a systemic ransomware attack lead to 2.4% GDP decline which illustrate the macroeconomic risks posed by insufficient cybersecurity(Cobos, 2024). For South African SMEs, similar vulnerabilities could lead to significant financial disruptions, emphasising the need for robust cybersecurity measures.

The adoption of advanced technologies such as the Internet of Things (IoT), Artificial Intelligence (AI), and smart systems has further complicated the

cybersecurity landscape(Kaur et al., 2023). While these technologies offer numerous benefits, they also introduce new vulnerabilities. For instance, the use of Industrial Control Systems (ICS) in manufacturing and mining operations exposes these industries to cyber threats that can disrupt operations and lead to catastrophic consequences (PWC, 2021).

Globally, ransomware remains one of the most common cyber threats. Ransomware attacks have targeted various industries, including aerospace, automotive, and healthcare, with significant financial impacts(Department for Science, 2024). In 2020, the manufacturing sector accounted for 17% of ransomware attacks, highlighting the critical need for robust cybersecurity measures (PWC, 2021).

Economic losses from cyber incidents, such as the 2.4% GDP decline in Costa Rica following a systemic ransomware attack, illustrate the macroeconomic risks posed by insufficient cybersecurity(Cobos, 2024). For South African SMEs, similar vulnerabilities could lead to significant financial disruptions, emphasising the need for robust cybersecurity measures.

The World Economic Forum released a reported in January ‘’*Global Cybersecurity Outlook 2025”,* which underscores the growing complexity in cyberspace, driven by interconnected supply chains, emerging technologies, and geopolitical tensions(World Economic Forum, 2025). These complexities exacerbate cyber inequity, widening the gap between large and small organisations(World Economic Forum, 2025) and it ties back to what PWC found in their 2020 report. SMEs, particularly in emerging economies like South Africa, face compounded challenges due to limited resources, skills shortages, and fragmented regulations. These findings align with existing literature that highlights SMEs vulnerability to advanced cyber threats and the need for targeted interventions to enhance their resilience.

Cybersecurity Threat Trends

Globally, SMEs are encountering a rising number of sophisticated cyber threats. According a report by Amrin, SMEs are increasingly targeted by cybercriminals due to their relatively weaker security infrastructures compared to larger enterprises(Amrin, 2014). These threats are not only becoming more frequent but also more complex, as attackers adopt advanced techniques such as machine learning and artificial intelligence to breach defences(Rawindaran et al., 2021). According to the 2024 Cyber Security Breaches Survey, medium and large organisations were more likely to be the subject of a cybersecurity breach or attack, with half of businesses and almost one-third of charities reporting such an incident in the previous 12 months (Department for Science, 2024).

The impact of cyber-attacks on SMEs can be devastating. Cyber incidents can result in significant financial losses, which frequently force businesses to close. Many SMEs are more vulnerable to long-term harm because they lack the means to recover from major cyber-attacks, according to a report on global trends (Naude et al., 2023). Furthermore, the reputational damage resulting from a breach can erode customer trust, which is crucial for the survival and growth of SMEs(Naude et al., 2023).

2.4 Local Landscape of SME Cybersecurity Threats

The cybersecurity landscape for SMEs in South Africa presents unique challenges shaped by the country's socio-economic and regulatory environment (PWC, 2021). This section examines the specific cybersecurity threats faced by South African SMEs, drawing on insights from various studies and reports.

In the South African context, the adoption of Fourth Industrial Revolution (4IR) technologies has been widespread, with 87% of business leaders acknowledging the competitive advantage provided by these technologies (PWC, 2021). However, the reliance on interconnected systems has also increased the risk of cyberattacks. The mining and manufacturing sectors in South Africa have been

quick to adopt smart technologies, but this has also made them prime targets for cybercriminals. Notable incidents include ransomware attacks that disrupted operations and resulted in significant financial losses (PWC, 2021).

Kenya presents a similar scenario, with SMEs in the e-commerce sector facing numerous cybersecurity challenges. A study on the cybersecurity assessment model for SMEs in Kenya's e-commerce sector revealed that the rapid growth of digital transactions has made these enterprises attractive targets for cybercriminals (Sang, 2023). The lack of cybersecurity awareness and inadequate defensive measures are major contributors to the vulnerability of Kenyan SMEs which is like South Africa.

The report on South African cybersecurity incidents highlights that the average cost of a data breach in South Africa is R49 million, placing the country as number fourteen globally among the countries that are hardest hit by such attacks. This underscores the financial strain cyber-attacks impose on SMEs, which may not have the resources to recover from such incidents(Puchert, 2024).

Unique Cybersecurity Challenges in South Africa

The socio-economic context in South Africa plays a significant role in shaping the cybersecurity landscape. Many SMEs operate with limited financial and technical resources, making it challenging to invest in robust cybersecurity measures. According to (Alexander, 2021), the economic constraints faced by South African SMEs often lead to underinvestment in cybersecurity, leaving them vulnerable to attacks.

South African SMEs must navigate a complex regulatory environment, including compliance with laws such as the Protection of Personal Information Act (POPIA)(UJ-TRCTI, 2022). Ensuring compliance can be resource-intensive and challenging for SMEs with limited expertise in cybersecurity and data protection (Alexander, 2021). Additionally, while SMEs in South Africa comply with POPIA, other countries must adhere to the General Data Protection Regulation

(GDPR)(Wolford). GDPR is Europe's comprehensive data privacy and security law, imposing numerous requirements on organisations worldwide to protect personal data(Wolford).This compliance requirement extends to third-party providers used by local SMEs, leading to the challenge of cross-border regulation. While this may seem trivial, it has significant implications, as demonstrated by major technology companies like Google, which only recently established data centres in South Africa to align with POPIA requirements. Prior to this, SMEs relying on cloud-based services such as Google Drive and Google Forms for data storage and customer information capture may have unknowingly been in breach of POPIA. This highlights the complexities of regulatory compliance for SMEs, as they must not only secure their own systems but also ensure that their third-party service providers adhere to local data protection laws.

Financial losses from cyber incidents can be debilitating as mentioned before in the global landscape, same applies locally as mentioned by (Alahmari & Duncan, 2020).The cost of recovering from a cyber-attack can be prohibitively high, often leading to business closure or significant operational disruptions (Alexander, 2021).

The rise in cyber-attacks targeting SMEs has increased significantly, with these businesses becoming more vulnerable due to their less stringent security measures and lower cybersecurity awareness among employees(Alharbi et al., 2021). Moreover, the high cost and complexity of implementing advanced cybersecurity solutions leave SMEs at a disadvantage, further exposing them to potential cyber threats (Aygun et al., 2022)

South Africa has witnessed several high-profile data breaches and ransomware incidents, which underscore the critical need for robust cybersecurity measures among SMEs. Incidents such as the ransomware attack on OneDayOnly and data breaches involving entities like TransUnion and Experian have demonstrated the severe consequences of inadequate cybersecurity practices(Puchert, 2024). These include financial losses, operational disruptions, and significant reputational damage, all of which threaten the

viability of affected businesses. Such examples emphasise the importance of implementing effective cybersecurity strategies to safeguard sensitive information and maintain stakeholder trust. The increasing frequency and sophistication of these attacks further highlight the urgent need for SMEs to strengthen their cybersecurity defences to mitigate risks and enhance resilience.

2.5 Sectors of Focus

Below section explains the reason behind the chosen sectors.

Financial Services

The financial services sector represents a significant target for cybercriminals, given the sensitive nature of the financial data and transactions managed by these entities. This sector's significant financial incentives render it especially susceptible to advanced cyber-attacks, thereby requiring rigorous cybersecurity protocols (PWC, 2021).

Retail and e-commerce

Retail and e-commerce are interconnected sectors that facilitate the buying and selling of goods and services through physical stores and online platforms, respectively. The retail and e-commerce sectors handle substantial amounts of personal and financial data, rendering them appealing targets for cybercriminals. According to (Department for Science, 2024),the rise of online shopping and digital transactions has intensified the demand for effective cybersecurity measures to safeguard customer data and uphold trust

.

Manufacturing

The manufacturing sector has experienced an increase in cyber-attacks aimed at industrial control systems and supply chains. Such attacks can interrupt production processes, resulting in substantial financial losses and operational delays. The sector's dependence on interconnected systems highlights the necessity for robust cybersecurity strategies (Department for Science, 2024).

Mining

The mining sector, critical to South Africa's economy, is increasingly targeted by cyber-attacks aimed at disrupting operations and stealing valuable proprietary data. The sector adoption of digital technologies and reliance on operational technology systems make it a prime target for cyber threats. Robust cybersecurity measures are essential to protect these critical infrastructures and ensure operational continuity(SEDA, 2023).

2.6 Common Cyber Attacks reported

In order to contextualise the cybersecurity dangers that SMEs faces, it is essential to name the often reported cyberattacks. Knowing the specific threats, like supply chain attacks, ransomware, and phishing helps draw attention to the real-world vulnerabilities that SMEs face and emphasises how urgent it is to implement strong cybersecurity technical measures. This part also supports the study's goal of analysing current cybersecurity procedures, determining how effective they are, and suggesting focused remedies to lessen these risks in the context of South African SMEs.

- **Phishing Attacks**: One of the most common risks is still phishing. Cybercriminals lure employees into disclosing private information, including login credentials and financial information, by using misleading

emails and websites. Phishing attacks are a constant threat to SMEs worldwide because of their efficacy in taking advantage of human weaknesses. According to the poll, 84% of enterprises and 83% of nonprofits reported that phishing was the most frequent kind of breach(Department for Science, 2024).

- **Malware and Ransomware-** Malware, including ransomware, poses a significant threat to SMEs(Alahmari & Duncan, 2021). Ransomware attacks, where cybercriminals encrypt company data and demand a ransom for its release, have seen a dramatic increase. A study done by Alexander in 2021 highlights that ransomware attacks on SMEs can cripple operations, leading to substantial financial losses and reputational damage (Alexander, 2021).
- **Insider Threats** -Insider threats, whether intentional or accidental, are another critical concern. Employees with access to sensitive information can inadvertently or maliciously compromise cybersecurity(Department for Science, 2024). These threats are challenging to detect and mitigate, as they originate from within the organisation.
- **Supply Chain Attacks-** SMEs are also vulnerable to supply chain attacks, where cybercriminals target less secure suppliers or partners to gain access to the primary target network(Department for Science, 2024). This type of attack underscores the importance of securing not only the SME's systems but also ensuring the security practices of their business partners. The survey notes an increasing awareness of supply chain risks, although many SMEs still lack formal procedures to manage these risks(Department for Science, 2024).
- **Vishing-** are a form of social engineering where attackers exploit voice communication channels, such as phone calls, to deceive individuals into sharing sensitive information or taking actions that jeopardise their security (Ashfaq et al., 2024). Vishing is highlighted in this study because it represents a growing cyber threat faced by SMEs. Given the increasing reliance on digital and voice-based communication channels within

SMEs, vishing attacks exploit these vulnerabilities to access sensitive information, posing significant risks to their operational and data security. Addressing vishing within the context of this research emphasises the need for comprehensive cybersecurity strategies tailored to the unique challenges faced by SMEs in South Africa.

Due to the increasing frequency and sophistication of cyberattacks, SMEs in South Africa are at danger. As highlighted, ransomware, phishing and social engineering remain dominant attack (PWC, 2021). (Alexander, 2021) agrees with PWC in that, ransomware attacks, which have severely impacted businesses globally, continue to cripple South African SMEs, leading to operational paralysis and financial losses. Furthermore, data breaches expose sensitive customer and business information, resulting in reputational damage and regulatory penalties(Kariuki et al., 2023). These threats reinforce the need for SMEs to adopt proactive technical cybersecurity measures, enhance employee awareness, and ensure compliance with data protection regulations to mitigate risks effectively.

2.7 Technical Cybersecurity Measures

As the initial line of protection, firewalls regulate incoming and outgoing network traffic according to preset security rules, making them essential parts of network security (Armenia, 2021). According to (Alahmari & Duncan, 2021) SMEs use firewalls to safeguard private information and preserve safe channels of communication, but the efficiency of these systems is highly dependent on appropriate setup and administration. In order to handle changing threats, Varachia also highlights the necessity of constant firewall configuration monitoring and updating (Varachia, 2022). A considerable portion of cyberattacks can be avoided by using firewalls that are configured correctly (Manzoor et al., 2024). However, the efficacy of firewalls in SMEs is often compromised by inadequate configuration and lack of regular updates (Manzoor et al., 2024). To guarantee consistent and current configurations, SMEs should implement automated firewall management solutions, according to (Bhattacharya, 2015).

Intrusion Detection Systems (IDS) are critical for monitoring network traffic and identifying potential threats(Manzoor et al., 2024) . IDS can be network-based (NIDS) or host-based (HIDS)(Manzoor et al., 2024). Research highlights that while many SMEs recognise the importance of IDS, the high rate of false positives and the resource constraints often limit their effective implementation (Cook, 2017). Additionally, the lack of skilled personnel to manage and interpret IDS alerts further complicates their use in SMEs (Alexander, 2021)IDS are effective in identifying suspicious activities, thus providing SMEs with critical time to respond to potential threats (Alahmari & Duncan, 2021). SMEs with IDS experience fewer successful breaches compared to those without such systems (Alahmari & Duncan, 2021). However, the high rate of false positives remains a challenge. Effective training and the implementation of machine learning algorithms can help reduce false positives and improve threat detection accuracy (Varachia, 2022).

Data confidentiality and integrity must be protected using encryption methods like SSL/TLS for data in transit and AES for data at rest (Yudhiyati & Putritama, 2021) . However, the deployment of these protocols varies across different industries, with financial and healthcare sectors showing higher implementation rates due to stricter regulatory requirements(Eybers & Mvundla, 2021). In South Africa, SMEs face challenges in deploying encryption protocols due to a lack of technical expertise(Cook, 2017). Encryption is crucial for compliance with data protection regulations, which is becoming increasingly important as cyber threats evolve (Varachia, 2022).Encryption significantly enhances data security by rendering data unreadable to unauthorised users(Amrin, 2014). SMEs using robust encryption protocols experience fewer data breaches. However, improper key management and outdated encryption standards hinder the effectiveness of encryption in SMEs (Alahmari & Duncan, 2021). The use of encryption must be accompanied by regular audits and updates to encryption methods to maintain their effectiveness against emerging threats(Alexander, 2021).

Endpoint security software protects individual devices from cyber threats(Renaud & Ophoff, 2021). This includes antivirus programs, anti-malware tools, and advanced threat protection solutions(Renaud & Ophoff, 2021). Research shows that SMEs are increasingly investing in endpoint security software to safeguard their digital assets, although the effectiveness of these solutions depends on regular updates and proper configuration(Alahmari & Duncan, 2021). (Ncubukezi, 2023) notes that regular updates are vital to combat the latest malware and exploit techniques. For devices to be safe from malware and other threats, endpoint security solutions are essential (Renaud & Ophoff, 2021). SMEs using comprehensive endpoint security software have lower incidences of malware infections. The efficiency of these solutions is dependent on regular updates and user compliance(Alahmari & Duncan, 2020) .Continuous education on the importance of these updates can significantly enhance the effectiveness of endpoint security measures (Varachia, 2022)

(Renaud & Ophoff, 2021) indicate that Security Information and Event Management (SIEM) solutions play a crucial role in enhancing the cybersecurity posture of SMEs by providing real-time analysis of security alerts generated by hardware and software applications. SIEM solutions aggregate and analyse data from various sources within an IT infrastructure, helping to detect, monitor, and respond to potential security incidents (Renaud & Ophoff, 2021).

These solutions are particularly beneficial for SMEs as they offer comprehensive visibility into network activities and facilitate the early detection of cyber threats. For example, SIEM systems can correlate data from firewalls, intrusion detection systems, and endpoint security tools to identify suspicious patterns that may indicate a security breach (Alahmari & Duncan, 2020)

Research indicates that the adoption of SIEM solutions among SMEs is growing, driven by the increasing need to comply with regulatory requirements and the desire to enhance overall security capabilities (Ncubukezi, 2023). However, the implementation and maintenance of SIEM solutions can be challenging for SMEs due to the complexity and cost associated with these

systems(Manzoor et al., 2024). Additionally, SMEs must navigate the choice between cloud-based and on-premises hosting, each with its own regulatory implications. While cloud-hosted SIEM solutions offer scalability and lower upfront costs, they raise concerns regarding data sovereignty and compliance with local regulations such as POPIA. On the other hand, on-premises solutions provide greater control over data storage and security but require significant investment in infrastructure and expertise. This decision further complicates the adoption of SIEM solutions for SMEs operating under resource constraints. Regular tuning and updates are necessary to ensure that SIEM solutions can effectively detect and respond to emerging threats. Part of this paper is to check within South Africa, if the adoption is growing, what are some of the challenges SMEs experience while they try to implement, see what a solution to that problem could be.

The list of technical measures listed above is not exhaustive, it is some of the most common ones. This paper sought to see which of the above measures do some of the SMEs in South Africa have and check how effective they are in protecting them.

2.8 Challenges Faced by SMEs in Implementing Cybersecurity Measures

High costs associated with advanced cybersecurity technologies and services deter many SMEs from adopting comprehensive cybersecurity measures(UJ-TRCTI, 2022). This financial constraint often leads to a reliance on basic or free cybersecurity tools, which may not provide adequate protection(Alahmari & Duncan, 2021) . Effective cybersecurity solutions require investment, and limited budgets can force SMEs to prioritise short-term costs over long-term security benefits (Alexander, 2021).

Many SMEs lack dedicated IT staff or cybersecurity professionals, which hinders the proper implementation and maintenance of cybersecurity measures(Chingoriwo, 2022). This skills gap results in improper configuration and underutilisation of available security tools(Yudhiyati & Putritama, 2021).The shortage of skilled cybersecurity professionals makes it difficult for SMEs to maintain a robust security posture (Chingoriwo, 2022). Talent shortages and financial constraints remain among the most significant challenges faced by SMEs in implementing effective cybersecurity measures. According to the Boston Consulting Group's annual cybersecurity survey, the shortage of qualified personnel limits the ability of SMEs to develop and maintain a robust cybersecurity posture(O'Niell et al., 2024). Additionally, competing financial priorities often leave SMEs with insufficient resources to invest in advanced security tools and technologies. These barriers exacerbate their vulnerability to cyber threats, as inadequate defences and limited expertise make it difficult to respond effectively to evolving cyber risks.

The complex regulatory environment poses a significant challenge for SMEs striving to implement effective cybersecurity measures. The World Economic Forum report highlights that the rapid pace of technological advancements often outpaces the development of regulatory frameworks, leading to governance gaps(Forum, 2024). This creates additional difficulties for SMEs that are already struggling to comply with existing regulations such as the Protection of Personal Information Act (POPIA) and the General Data Protection Regulation (GDPR)(Forum, 2024). Navigating these regulatory complexities requires resources and expertise that many SMEs lack, further compounding their challenges in achieving compliance and maintaining a robust cybersecurity posture.

Awareness of cybersecurity threats and the importance of robust security measures is often low among SME owners and employees(Kariuki et al., 2023). This lack of awareness contributes to inadequate cybersecurity practices and increases vulnerability to cyber-attacks (Kariuki et al., 2023). Ongoing training

and awareness programs are essential for improving cybersecurity posture in SMEs(Yudhiyati & Putritama, 2021) . Regular training sessions and awareness campaigns can significantly reduce the risk of human error and improve overall security (Alexander, 2021). Addressing these challenges is critical for SMEs to build resilience and protect their digital assets(O'Niell et al., 2024).

2.9 Existing best practices for Cybersecurity Solutions within SMEs

Adopting open-source tools, cloud-based security services, and managed security service providers (MSSPs) are viable options for SMEs with limited budgets(UJ-TRCTI, 2022). These alternatives can provide robust security features without the high upfront costs associated with traditional security infrastructure(Yudhiyati & Putritama, 2021). Leveraging community resources and government-supported cybersecurity initiatives can also offer cost-effective solutions for SMEs(Alexander, 2021).

Investing in skill development through training programs and certifications can bridge the technical expertise gap within SMEs (Rawindaran et al., 2023). Outsourcing cybersecurity functions to third-party experts or MSSPs can enhance the security posture of SMEs by leveraging specialised knowledge and resources (Alahmari & Duncan, 2021) .Building partnerships with educational institutions can also help SMEs access skilled cybersecurity professionals(Alexander, 2021)

Promoting cybersecurity awareness and fostering a culture of security within SMEs is essential(Renaud & Ophoff, 2021). Regular training sessions, awareness campaigns, and the establishment of cybersecurity policies can significantly improve the overall security readiness of SMEs(Eybers & Mvundla, 2021). A proactive approach to cybersecurity culture can lead to better compliance and more effective use of security tools(Yudhiyati & Putritama, 2021) . Implementing regular cybersecurity drills and simulations can further reinforce

a culture of security awareness(Alexander, 2021). Additionally, (Lloyd, 2020) emphasises that incorporating cybersecurity awareness into the core values of the company can result in a more resilient and security-conscious workforce.

2.10 Key Themes from the literature

This section presents key themes identified from the literature review on cybersecurity challenges and best practices for SMEs. These themes are derived from existing research, theoretical models, and global cybersecurity frameworks, offering insights into the factors influencing cybersecurity adoption, barriers to implementation, and strategies for improving resilience.

In Chapter 4, the study will introduce key themes emerging from the research findings, based on the experiences and perspectives of SMEs that participated in this study. These empirical insights will provide a real-world perspective on how SMEs approach cybersecurity, the challenges they face, and the strategies they employ.

In Chapter 5, the themes from literature and research findings will be compared and analysed to assess their alignment or divergence. This comparative approach will help identify gaps between academic knowledge and practical implementation, highlighting areas where SMEs require additional support, whether through financial assistance, policy interventions, or enhanced cybersecurity awareness.

The following diagram represents the key themes identified from the literature, which will later serve as a basis for comparison with the research findings.

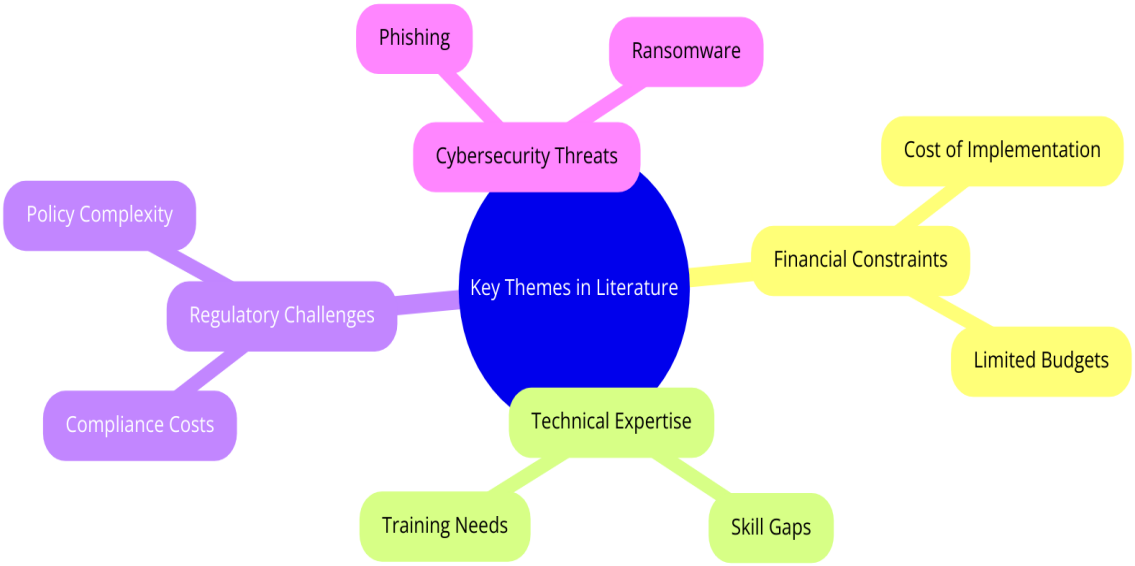


Figure 2-1 The diagram illustrates some of the interesting themes emerging from literature. Let us see in the next chapters if this paper will find similarities based on SMEs in the South African context.

2.11 Analytical Framework

By combining the theoretical and empirical ideas, the analytical framework offers a methodical way to comprehend the phenomena being studied. The theoretical underpinnings that underpin this study on the adoption of technical cybersecurity measures in SMEs in the South African market are described in this section.

Theoretical Framework

A theoretical framework gives a research study its fundamental structure by establishing theories that have been proven correct by earlier studies. To comprehend the implementation and efficacy of technical cybersecurity measures in SMEs, this study makes use of the Resource-Based View (RBV), Diffusion of Innovations (DOI) Theory, and Technology Acceptance Model (TAM). Previous studies have shown that these models are applicable to cybersecurity-related research. For example, (Fallatah et al., 2024) investigated the Technology

Acceptance Model (TAM) in the context of cybersecurity training, looking at how user acceptance of security practices is influenced by elements including perceived usefulness and simplicity of use. According to their research, user involvement, trust, and compliance, all of which are crucial components of cybersecurity adoption, are necessary for training to be effective. Similarly, (Cruz et al., 2024) integrated Diffusion of Innovations (DOI) Theory and RBV to examine the implementation success of cybersecurity data analytics systems (CDAS) in government organisations. Their study found that compatibility, trialability, internal processes, and organisational learning significantly influence the success of cybersecurity systems.

The inclusion of TAM, DOI, and RBV in this study aligns with this earlier research by providing a structured approach to evaluating cybersecurity adoption in SMEs. TAM helps assess user behaviour toward cybersecurity measures, DOI aids in understanding how cybersecurity innovations spread among SMEs, and RBV provides a strategic lens to evaluate how cybersecurity capabilities contribute to a firm's competitive advantage. By leveraging these established models, this study ensures a comprehensive analysis of the factors driving cybersecurity adoption in SMEs, contributing to both academic knowledge and practical cybersecurity improvements.

- **Technology Acceptance Model (TAM):** Developed by Davis in 1989, TAM explains how users come to accept and use technology (Kansal & Saha, 2023). It posits that perceived usefulness and perceived ease of use are the primary factors influencing technology adoption. In the context of this study, TAM helps explain the factors influencing SMEs decisions to implement specific technical cybersecurity measures.

- **Diffusion of Innovations Theory:** Proposed by Rogers in 1962,this theory describes how innovations are adopted over time (Wonglimpiyarat & Yuberk, 2005). In the context of this paper, it provides insights into how SMEs adopt new cybersecurity measures and the factors that influence their decisions.

- **Resource-Based View (RBV):** This theory emphasises the importance of internal resources in gaining and maintaining a competitive advantage(Münter, 2024). In the context of this study, RBV helps understand how financial capacity, technical expertise, and organisational support influence the implementation of cybersecurity measures in SMEs.

2.12 Conclusion of Literature Review

Several important insights and gaps have been highlighted as a result of the literature review on the application of technical cybersecurity measures within SMEs in the South African market. One of the most significant gaps was the lack of sector-specific cybersecurity research on SMEs in South Africa. While global studies highlighted broad challenges faced by SMEs, there was limited empirical research that addressed how these challenges manifested within specific industries such as retail, manufacturing, mining, and financial services. Understanding these sectoral differences was crucial for developing tailored cybersecurity interventions. Another gap was the absence of studies examining how SMEs navigate financial and resource constraints when adopting cybersecurity solutions. Literature did acknowledge that budget limitations hinder cybersecurity implementation, but there is little research on how SMEs prioritise security investments or leverage cost-effective solutions. This study aimed to bridge that gap by investigating alternative approaches SMEs use to enhance their cybersecurity posture despite financial constraints.

There were little discussion of how regulatory compliance affects SMEs' cybersecurity tactics, according to the literature review. Security requirements are shaped by international standards like GDPR and laws like POPIA, but little is known about how SMEs understand and apply these laws or how compliance constraints affect their day-to-day operations. Further research is still needed on the legislative obstacles that SMEs must overcome, particularly those that use third-party cloud services and must contend with international data protection regulations. This study sought to close these gaps and offer a more thorough,

industry-specific, and solution-focused understanding of the cybersecurity possibilities and difficulties that South African SMEs face. The results will benefit academia and industry by providing useful suggestions catered to the limitations and regulatory framework of SMEs.

The research emphasises how crucial it is for SMEs around the world to have strong cybersecurity defences against a range of advanced cyberthreats, including ransomware, malware, and phishing. In addition to posing serious financial concerns, these dangers endanger business continuity and harm reputations.

The literature highlights the critical importance of robust cybersecurity measures for SMEs globally, emphasising their vulnerability to a variety of sophisticated cyber threats such as phishing, malware, and ransomware. These threats not only pose significant financial risks but also jeopardise operational continuity and damage reputations.

Locally, in South Africa, SMEs face unique challenges including limited financial resources, technical expertise gaps, and compliance with regulatory frameworks such as the Protection of Personal Information Act (POPIA). These factors contribute to the complexity of implementing effective cybersecurity strategies tailored to the specific needs and constraints of SMEs in the region.

The literature review also underscores various best practices and solutions available to SMEs, such as leveraging cost-effective cybersecurity tools, outsourcing security functions to managed service providers, and enhancing cybersecurity awareness and training programs. These practices aim to mitigate risks and strengthen SMEs cybersecurity posture amidst evolving cyber threats and technological advancements.

This study sought to contribute to the existing body of knowledge by exploring the current state of technical cybersecurity implementation in South African SMEs. By examining factors influencing adoption and effectiveness, including the role of regulatory compliance, financial constraints, and organisational culture,

this research aimed to provide actionable insights and recommendations for enhancing cybersecurity resilience within the SME sector.

To guide the empirical investigation, this study identified a set of key propositions derived from the literature and theoretical frameworks. These propositions serve as anchors for analysing the findings and are summarised in Table 2.1 below.

Proposition	**Description**	**Linked Theory**
P1	SMEs with stronger internal capabilities are more likely to implement advanced cybersecurity tools.	RBV
P2	Regulatory pressure influences the adoption of cybersecurity practices among SMEs.	DOI
P3	SMEs perceive cybersecurity tools as difficult to use and costly, hindering adoption.	TAM
P4	Industry-specific risk profiles impact the type of cybersecurity solutions adopted.	RBV & DOI
P5	External support and managed services positively influence cybersecurity resilience.	RBV & TAM

Table 2.1: Summary of Propositions

CHAPTER 3. RESEARCH METHODOLOGY

This chapter outlines the research methodology used to examine the propositions presented in Chapter 2. It details the research paradigm, research approach, design, and data collection instruments employed in the study. The chapter concludes with a discussion on the transferability, credibility, and dependability of the study.

3.1 Research Paradigm

Interpretivism has been selected as the research paradigm for this investigation. The foundation of interpretivism is the conviction that social actors create reality, which can only be fully comprehended by applying meanings and interpretations to personal experiences. This paradigm was in line with the study's objective, which was to investigate and comprehend the intricate, situational, and individualised experiences of SMEs when putting cybersecurity measures into place.

Ontology, epistemology, and axiology collectively shape how individuals perceive, understand, and interact with the world. Ontology, the study of being and reality, determines how one sees and views the world, influencing beliefs about what exists and what is possible(Aliyu et al., 2015). For instance, a realist ontology assumes that the world exists independently of our perceptions, while a constructivist ontology suggests that reality is constructed through human experiences and social interactions(Aliyu et al., 2015). This research assumes a constructivist ontology, recognising that the cybersecurity practices of SMEs are influenced by social and cultural factors specific to their context.

Epistemology, the study of knowledge, addresses how one thinks about the world and what constitutes valid knowledge(Aliyu et al., 2015). It encompasses the methods and justifications for acquiring knowledge, such as empirical

observation, logical reasoning, or subjective interpretation(Aliyu et al., 2015). Different epistemological positions, such as positivism or interpretivism, guide how researchers investigate and interpret phenomena. In this study, the epistemology emphasises understanding phenomena through the meanings that participants attach to them, seeking to uncover how SMEs make decisions about security and experience challenges specific to their context.

Axiology, the study of values, concerns how one acts in the world, guiding ethical considerations and judgments about what is important or worthwhile(Aliyu et al., 2015). It influences decision-making processes, prioritisation of goals, and the ethical standards upheld in both personal and professional contexts. Axiology in this context acknowledges the values and biases of both the researcher and the participants as part of the research process(Aliyu et al., 2015). This perspective ensures that the study is conducted with a deep understanding and respect for the values and ethical considerations relevant to SMEs and their cybersecurity practices.

Together, these philosophical foundations inform the interpretivist approach of this research, shaping the methodology and analysis to provide a rich, contextualised understanding of the technical implementation of cybersecurity measures within South African SMEs.

3.2 Research approach

This study used a qualitative research approach, which is suitable for exploring the depth and complexity of SMEs experiences with cybersecurity measures. Qualitative research allowed for a detailed understanding of the phenomena under investigation, providing rich, contextual, and nuanced data (Aliyu et al., 2015). A mixed-method or quantitative approach was not chosen because, while they might capture broad trends such as percentage of SMEs with specific cybersecurity technologies, they would not reveal the underlying rationale behind these decisions or the challenges influencing cybersecurity adoption. This

approach was well-suited to answer the research objectives, as it focused on understanding the "how" and "why" of the cybersecurity measures employed by SMEs and the challenges they face.

3.3 Research Design and Justification

The research design for this study was a generic qualitative research design. The focus was on in-depth thematic exploration across multiple SMEs.

The research was conducted through physical and virtual one-on-one interviews using semi-structured questions to gain insights into the technical implementation of cybersecurity measures within South African SMEs across selected sectors. This approach enabled an in-depth exploration of participants experiences, challenges, and perspectives regarding cybersecurity practices, the effectiveness of current measures, and the specific obstacles they encounter.

To further support and triangulate the interview findings, relevant internal documentation such as incident reports, cybersecurity policies, and threat response records was also viewed from some of the participating SMEs. This document analysis provided additional context and validation for the insights obtained from interview participants, allowing for a more comprehensive understanding of the cybersecurity landscape within South African SMEs.

3.4 Data collection methods

Data was collected through semi-structured interviews and document analysis. Semi-structured interviews are chosen because they provide a balance between structured and open-ended questions, allowing for flexibility in probing deeper into specific areas of interest. Document analysis involved reviewing relevant documents such as cybersecurity policies, incident reports, and training materials

to triangulate the data collected from interviews and provide a comprehensive understanding of the cybersecurity practices in SMEs.

To validate the findings, several strategies were employed:

1. Triangulating data from multiple sources, including semi-structured interviews and document analysis, enhanced the credibility and reliability of the findings. Comparing and contrasting information obtained through different methods helps to corroborate and validate the results.
2. After data analysis, participants were invited to review summaries or interpretations of their responses to ensure accuracy and alignment with their experiences and perspectives. This process enhanced the dependability of the findings by incorporating participant's feedback.
3. There was engagement with colleagues and peers who are familiar with qualitative research methods and the topic to provide an external perspective on the analysis process and interpretations. This helped to ensure that bias was minimised and that interpretations become well-grounded in the data.

3.5 Population and sample

3.5.1 *Population*

The population for this study included SMEs operating in various sectors within the South African market.

3.5.2 *Sample and sampling method.*

A purposive sampling method was used to select SMEs that have implemented some form of cybersecurity measures. This method was ideal for qualitative

research as it allowed for the selection of information-rich cases that can provide detailed insights.

The sample focused on SMEs from the following sectors:

1. Financial Services

   Due to the high value of financial data and the frequent targeting of financial institutions by cybercriminals(Akhtar et al., 2021). Financial services companies are often prime targets for cyber-attacks because of the sensitive and valuable data they handle, making robust cybersecurity measures crucial(Akhtar et al., 2021).
2. Retail and e-commerce

   Due to the volume of personal and financial information processed and stored(Sang, 2023). These businesses are attractive targets for cybercriminals seeking to exploit customer data, and effective cybersecurity practices are essential to protect against breaches and maintain consumer trust(Sang, 2023).

3. Manufacturing

   There rise in cyber-attacks targeting industrial systems and supply chains (PWC, 2021). Cyber threats in manufacturing can lead to significant disruptions, operational downtime, and financial losses, highlighting the need for strong cybersecurity defences to protect critical infrastructure and intellectual property(PWC, 2021).
4. Mining

   Due to the critical nature of the industry and its increasing reliance on digital technologies. The mining sector faces unique cybersecurity challenges as it integrates advanced technologies such as automation, IoT, and data analytics(PWC, 2021). Cyber-attacks on mining operations can have severe consequences, including safety risks, environmental

hazards, and substantial financial losses, making cybersecurity a priority for maintaining operational integrity and safety(PWC, 2021).

The planned sample size was fifteen to twenty SMEs, selected using purposive sampling to ensure that participants had relevant experience with cybersecurity implementation. This approach allowed for a focused exploration of cybersecurity challenges and strategies within SMEs that actively engage with cybersecurity issues, ensuring that the findings were rich and contextually relevant. In total, thirteen SMEs were interviewed, providing valuable insights into the varying levels of cybersecurity adoption and the challenges faced across different sectors. The rationale for concluding the sample at thirteen participants, rather than the initially planned fifteen to twenty, is discussed in Chapter 4. Participants included SME owners, IT managers, and cybersecurity professionals. Thirteen SMEs were interviewed, eight of which had something in place which will be discussed in the next few chapters and five of the thirteen did not have anything in place but their responses to why they did not have was also valuable for the study hence they were included. In addition to the thirteen SMEs, two professionals were interviewed. Some of the people who were on the thirteen were cybersecurity professionals hence the study did not need more professionals to comment on the research.

Participants were selected based on their roles and expertise in managing and implementing cybersecurity measures within their organisations. The aim was to interview two to five professionals per sector to gather diverse perspectives, and the number of people interviewed per sector was achieved. This approach ensured a representative sample that reflects the various challenges and strategies employed across different industries.

The sampling process involved reaching out to potential participants via email to explain the study and request their participation. Once participants agreed, interviews were then scheduled at their convenience. This approach was designed to respect the participants availability and ensure their willingness to share their experiences.

The data collection instrument for this research included semi-structured interviews with open-ended questions aimed at soliciting the participants views, experiences, and opinions on cybersecurity measures in their organisations. Document analysis was also be conducted to validate and corroborate the findings from the interviews. Only four of the eight SMEs that had something in place were able to shed some light into the documentation, though they did not share actual documents.

This sampling method and approach ensured that the study captures a wide range of insights and experiences, providing a rich understanding of cybersecurity practices within SMEs across different sectors.

The sample was selected based on sector diversity, company size within SME definitions, and willingness to participate in a full interview process. While a sample size of thirteen SMEs provided rich insights, future studies may benefit from a larger or more geographically varied sample for broader generalisation.

3.6 The research instrument

The primary research instrument was an interview guide, which includes questions aligned with the research objectives:

1. Questions about the specific technical cybersecurity measures currently deployed and assessing the effectiveness of these measures.
2. Questions identifying challenges in implementing and maintaining cybersecurity measures.
3. Questions exploring strategies and best practices for optimising cybersecurity measures.

The interviews aimed to minimise bias and use simple terms for the participants to understand and a glossary of definitions was provided.

An example of the interview guide is included in the Appendix.

3.7 Procedure for data collection

Data was collected through face-to-face and virtual interviews, depending on the preferences and availability of the participants. SMEs were contacted directly to request participation in the study. Using a snowball sampling technique, the researcher sent a comprehensive email detailing the research to colleagues who subsequently pass it to pertinent SMEs. These SMEs, in turn, recommended others within their network, expanding the participant pool. This approach ensured diversity across sectors and company sizes, allowing for a broader representation of cybersecurity practices within South African SMEs. Interviews were scheduled at convenient times for the participants and conducted in a manner that ensures privacy and confidentiality. The aim was for all interviews to be audio-recorded (with participant consent) and transcribed verbatim for analysis, but not all participants were willing to be recorded due to the sensitivity around business and cybersecurity. In such cases, detailed notes were taken through active listening, ensuring key points were accurately documented. Additionally, post-interview reflections were conducted to capture any overlooked insights, and responses were shared with participants for validation, allowing them to confirm the information and add any details that may have been omitted. Participants were provided with the interview guide and ethical clearance form beforehand. They participants were informed about the recording process and assurance was provided that they can stop the interview at any point if they feel uncomfortable.

During the interview process, there was a request to access relevant documents, such as cybersecurity policies, incident reports, and training materials. However, due to confidentiality concerns, these documents were not physically shared with the interviewer. Instead, participants provided verbal summaries of their contents, highlighting key security measures, past incidents, and training efforts. In some cases, screen-sharing was used during virtual interviews to briefly showcase logs or policies without transferring files. This approach allowed the researcher to verify alignment between documented policies and participants stated

cybersecurity practices while maintaining data confidentiality. To ensure confidentiality and assure participants of the secure handling of these documents, the following steps will be taken:

1. Explanation of Purpose
   The purpose why the documents are requested was clearly explained, emphasising that the aim was to corroborate interview findings and gain a comprehensive understanding of the cybersecurity practices within the SME.
2. Confidentiality Assurance
   Assurance was provided to participants that all documents will be treated with the utmost confidentiality. Any sensitive information will be anonymised to protect the identity of the SME and its employees.
3. Secure Handling and Storage
   Participants were informed about the measures in place to securely handle and store the documents. This included encrypted digital storage and secure physical storage for any hard copies.
4. Informed Consent
   Participants were asked to sign a consent form, ensuring that they understand the purpose, procedures, and confidentiality measures associated with this part of the data collection process.
5. Option to Decline
   Participants were informed that providing documents is voluntary and that they can decline this request without any negative consequences for their participation in the interview.

3.8 Data analysis strategies and interpretation

Data analysis was conducted using reflexive thematic analysis, which involves identifying, analysing, and reporting patterns (themes) within the data(Clarke & Braun, 2017). Reflexive thematic analysis was appropriate for this qualitative research as it provided a flexible and systematic approach to data analysis(Clarke

& Braun, 2017). The steps included familiarisation with the data, coding, theme development, and interpretation(Clarke & Braun, 2017). A university-approved software, Atlas.ti, was used to assist with data management and analysis. This software was chosen due to its ability to efficiently organise, code, and categorise qualitative data, allowing for systematic identification of patterns and themes. Atlas.ti also facilitates thematic analysis by enabling the visualisation of connections between codes, assisting in the development of a coherent narrative from the findings. Additionally, it improves data reliability by ensuring consistency in coding across multiple responses, making it a valuable tool for qualitative research. This method emphasised the active role of the researcher in the analytical process, aligning well with the exploratory nature of this study on cybersecurity measures in SMEs. Reflexive thematic analysis offered flexibility and depth, enabling adaptation to the unique context of SMEs in South Africa and capturing specific nuances of their cybersecurity challenges and practices. It allowed for incorporating the researcher's insights and experiences into the data interpretation, leading to richer and more meaningful findings. The iterative nature of reflexive thematic analysis aligns with the exploratory nature of this study, allowing for continuous engagement with the data to refine themes and interpretations. Furthermore, it enables exploration of multiple layers of meaning, addressing both technical aspects and contextual factors influencing cybersecurity implementation and effectiveness.

Steps for Using Reflexive Thematic Analysis:

1. **Familiarisation with the Data:**
    - Transcribe the interviews verbatim.
    - Read and re-read the transcripts to become deeply familiar with the content.
    - Note any initial ideas or observations.
2. **Generating Initial Codes:**

- Systematically code interesting features of the data across the entire dataset.
- Use a university-approved software to assist with data management and coding.
- Collate data relevant to each code.

3. **Searching for Themes:**

    - Group codes into potential themes.
    - Gather all data relevant to each potential theme.
    - Reflect on how these themes relate to the research objectives.

4. **Reviewing Themes:**

    - Check if the themes work in relation to the coded extracts and the entire dataset.
    - Refine themes to ensure coherence and consistency.
    - Develop a thematic map to visualise the relationships between themes.

5. **Defining and Naming Themes:**

    - Clearly define each theme and the aspects of the data it captures.
    - Generate clear definitions and names for each theme.
    - Ensure themes are distinct and do not overlap excessively.

6. **Writing the Report:**

    - Weave the themes into a narrative that addresses the research objectives.
    - Include vivid examples and quotations to illustrate each theme.
    - Interpret the findings in the context of existing literature and theoretical frameworks.

3.9 Possible limitations and challenges of the study

- Findings from the study may not be generalisable to all SMEs due to the qualitative nature and the specific context of South Africa, resulting in limited generalisation.
- Participants may have provided socially desirable responses, particularly on sensitive topics such as cybersecurity practices resulting in bias.
- The collected data may have been influenced by the phrasing of certain questions, which included some that could have been leading.

While the study provided deep qualitative insights, its findings were limited by sample size and reliance on self-reported data. There may be response or social desirability bias during interviews. Triangulation with internal documentation aimed to mitigate this, but future studies could include independent cybersecurity assessments or observations.

3.10 Self-Reflexivity

Having worked as a telecommunications specialist creating technology solutions for companies, my background presents both benefits and possible prejudices that affect this study. My knowledge of cybersecurity solutions and their application helps one to have a complex awareness of technological ideas and pragmatic difficulties experienced by SMEs. This knowledge helps me to more precisely spot cybersecurity practice flaws, ask intelligent questions, and interpret technical answers. But it also runs the danger of bias as my professional background could lead to presumptions on the knowledge and skills of SMEs or

the apparent success of particular solutions. I took a methodical and open-ended approach to data collecting, letting participants share their individual viewpoints free from too directed guidance from my biases, therefore reducing this This reflective awareness guaranteed that the study stayed anchored in the reality and experiences of the SMEs, instead of being unduly shaped by my professional viewpoint.

3.11 Quality Assurance

3.11.1 *External validity OR transferability*

Transferability

Transferability refers to the extent to which the findings of qualitative research can be applied or generalised to other contexts, settings, or populations(Korstjens & Moser, 2017). Transferability in the context of this paper refers to the extent to which the findings of this study on cybersecurity measures within South African SMEs can be applied in other contexts. This is supported by clearly defining the context of the study and using purposive sampling, which specifically targets SMEs in sectors vulnerable to cyber threats, such as Financial Services, Retail and E-commerce, Manufacturing, and Mining. By focusing on these sectors, the study provides insights that can be relevant to similar SME environments both within and outside of South Africa, particularly in areas facing comparable cybersecurity challenges.

The purposive sampling method was chosen to capture diverse perspectives from IT managers, business owners, and cybersecurity professionals across these sectors. This approach enhanced transferability by selecting participants most likely to provide relevant information on cybersecurity practices, challenges, and mitigation strategies in SMEs, thus supporting the applicability of findings to other SME settings with similar risk profiles and resource constraints.

3.11.2 *Internal validity OR credibility*

Credibility

Credibility refers to the trustworthiness and believability of research findings. It ensures that the findings accurately reflect the information derived from participants original data and correctly interpret their perspectives(Korstjens & Moser, 2017). Credibility was ensured through member checking, where participants reviewed and verified the accuracy of the interview transcripts and the findings. Triangulation of data from interviews and document analysis also enhanced credibility.

3.11.3 *Reliability OR dependability*

Dependability

Dependability refers to the consistency and reliability of research findings over time(Korstjens & Moser, 2017). It ensures that the interpretations and recommendations derived from the study align with the data collected directly from participants, thereby supporting the credibility of the study (Korstjens & Moser, 2017). Dependability was achieved by maintaining a detailed audit trail of the research process, including data collection and analysis procedures, to allow for replication of the study.

3.12 Ethical considerations

3.11.1 Informed Consent

Informed consent is a cornerstone of ethical research practice. Participants were provided with a detailed explanation of the study, including its purpose, the procedures involved, and their rights as participants. They were informed about the voluntary nature of their participation and their right to withdraw from the study at any time without any negative consequences. Consent forms were used to

document their agreement to participate, and additional consent was obtained for the audio recording of interviews and for accessing relevant documents.

3.11.2 Confidentiality and Anonymity

Maintaining the confidentiality and anonymity of participants is paramount. All identifying information were anonymised during the transcription and analysis of the data. Pseudonyms were used to replace real names, and any specific details that could reveal the identity of the participants or their organisations were altered. Confidential documents provided by participants, such as cybersecurity policies and incident reports, are securely handled and stored. The researcher has employed encrypted digital storage for electronic files and locked cabinets for physical documents to ensure that all data remains confidential.

3.11.3 Data Security

Data security is critical to protecting the integrity and confidentiality of the research data. All digital data, including interview recordings and transcriptions, have been stored on an encrypted device, and backed up to secure, encrypted cloud storage. Physical documents have been stored in a locked cabinet with restricted access. Only the researcher has access to the data, ensuring that it remains secure throughout the research process.

3.11.4 Ethical Approval

Before commencing data collection, ethical approval was sought from the relevant institutional review board. This process involved a thorough review of the research proposal to ensure that all ethical considerations have been addressed and that the study complied with institutional and national ethical guidelines. The ethical review assessed the potential risks and benefits, the adequacy of the informed consent process, and the measures in place to protect participant confidentiality and data security. After going through the process as outlined by the university, ethical clearance was obtained and data collection began, which

ensured that the research adhered to the highest ethical standards. The transcript from the interviews were not made public.

3.12 **Conceptual Model**

The conceptual model proposed for this study combines key theoretical constructs and variables to examine the technical implementation of cybersecurity measures in South African SMEs. Drawing on the Technology Acceptance Model (TAM), Diffusion of Innovations Theory, and Resource-Based View (RBV), the model outlines the relationships between financial constraints, technical expertise, and regulatory pressures (independent variables) and their influence on the adoption and effectiveness of cybersecurity measures (dependent variables). The model also incorporates awareness of cybersecurity risks as an intervening variable, acknowledging its critical role in bridging resource limitations and the adoption of technical solutions. This framework provides a structured approach to understanding how SMEs navigate cybersecurity challenges and serves as a basis for analysing empirical findings.

Below is figure 3.1, The conceptual model, grounded in literature illustrates the key factors influencing SME cybersecurity adoption by integrating insights from established frameworks and prior to conducting research. It represents the relationships between financial constraints, expertise, regulatory compliance, and technological readiness as critical determinants of cybersecurity resilience. This model provides a structured foundation for analysing how these elements interact and shape SMEs ability to implement and sustain effective cybersecurity measures.

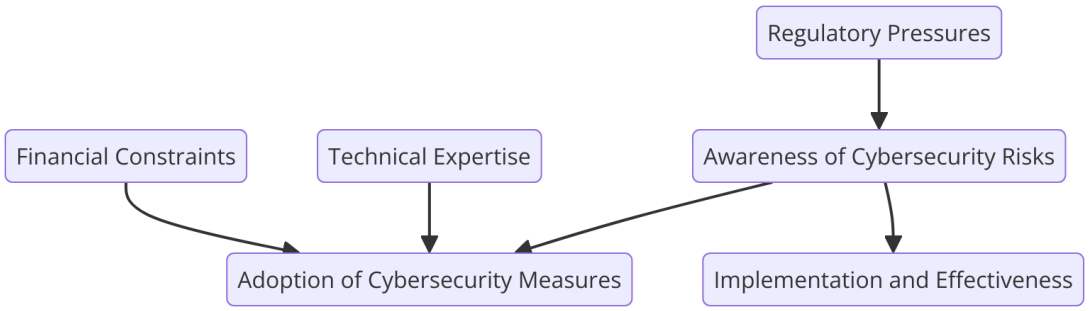


Figure 3-1: The conceptual model, grounded in literature.

CHAPTER 4. FINDINGS AND ANALYSIS

4.1 Introduction

This chapter summarises the study's findings, which are organised to meet the goals of the investigation and provide light on South African SMEs cybersecurity procedures. The focus is on identifying current technical cybersecurity measures, evaluating their effectiveness, and understanding the challenges faced by SMEs in implementing and maintaining these technical measures.

The data gathered from interviews with SMEs in South Africa's manufacturing, mining, retail and e-commerce, and financial services industries is analysed in this chapter.

Chapter four focuses on presenting the findings and analysis of the data collected from participating SMEs. The findings are presented in an objective manner, with emphasis on identifying patterns and trends within the data. Importantly, this chapter does not discuss the broader implications of these findings; will be for Chapter five, where the results will be critically evaluated and contextualised in relation to the research objectives and existing literature.

The thematic analysis approach was used to identify key themes and insights from the interviews. The findings are organised according to the main themes derived from the research objectives, which include current cybersecurity measures, challenges faced, and strategies for improving cybersecurity practices.

4.2 Background for Participants and Companies

4.2.1 *Overview of Participants*

Through one-on-one interviews, thirteen SMEs took part in the study. The duration of the interviews varied depending on whether the participant indicated that their organisation had implemented any cybersecurity measures or lacked such measures entirely. The interviews ranged from 18 minutes to 56 minutes. The original proposal aimed for a sample of fifteen to twenty SMEs. After obtaining ethical clearance, thirteen participants were interviewed. Given the goal of qualitative research is not statistical generalisability but rather to gain an in-depth, contextual understanding of the phenomenon, this sample size was sufficient to reach saturation.

The participants were across different sectors, which is Financial Services, Retail and e-commerce, Manufacturing and Mining.

The sectors that are represented in the study are shown graphically below.

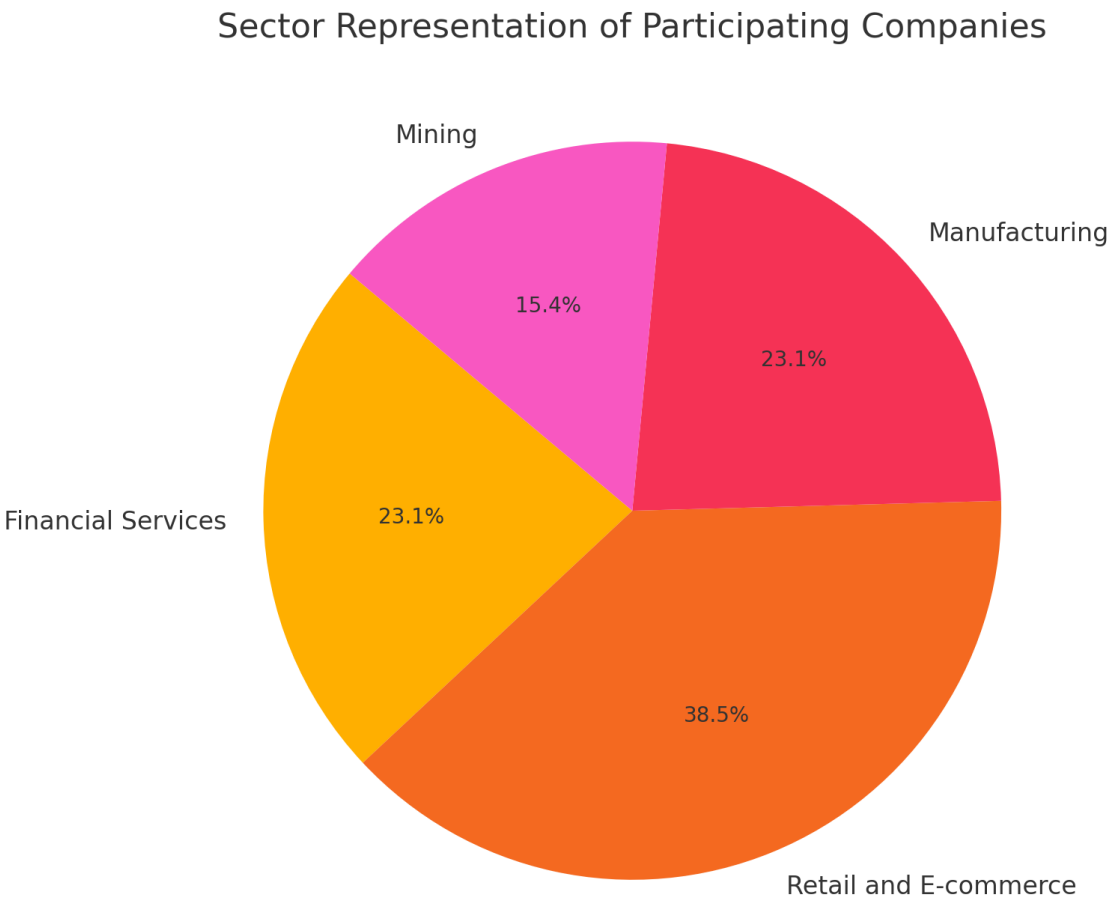


Figure 4-1: The sectors representation of participating companies offers an overview of the industries included in the study, highlighting the distribution of SMEs across key sectors such as financial services, retail & e-commerce, manufacturing, and mining, to contextualise their cybersecurity challenges and readiness.

The study included thirteen SMEs across four key sectors:

- Financial Services - Three interviews were conducted for this sector
- Retail and e-commerce – five interviews

- Manufacturing – Three interviews, and finally
- Mining - two interviews

Among the participating SMEs, five had minimal or no cybersecurity measures in place, while the remaining eight demonstrated varying levels of cybersecurity implementation, ranging from basic security controls to more advanced technical measures.

The following table provides an overview of the participants, including their roles within their organisations, company size, and industry sector.

Participant ID	Position	Size of SME	Sector
Participant 1	Owner	Small	Financial Services
Participant 2	IT Manager	Medium	Retail and e-commerce
Participant 3	Cybersecurity Consultant	Medium	Manufacturing
Participant 4	Owner	Small	Mining
Participant 5	IT Specialist	Medium	Retail and e-commerce
Participant 6	General Manager	Small	Financial Services
Participant 7	Owner	Small	Retail and e-commerce
Participant 8	IT Manager	Medium	Retail and e-commerce
Participant 9	Security Officer	Small	Manufacturing
Participant 10	Owner	Small	Mining
Participant 11	Operations Manager	Medium	Retail and e-commerce
Participant 12	IT Consultant	Medium	Financial Services

Participant 13	Technical Lead	Medium	Manufacturing

Table 4-1: Overview of Participants

4.2.2 *An Overview of Companies Involved.*

This section provides an overview of the companies interviewed within the financial services, retail and e-commerce, manufacturing, and mining sectors. By understanding the nature of these businesses, we can better assess the importance of cybersecurity in safeguarding their operations and sensitive data against evolving cyber threats. The following outlines the core activities of the companies interviewed and highlights the relevance of cybersecurity in these sectors.

- **Financial Services**
  Three companies were interviewed in the financial services sector, and these companies operate in various areas of financial management, including payment processing, micro-lending etc. These companies deal with highly sensitive financial data, such as customer account information, payment details, and transaction histories. Maintaining the secrecy, integrity, and data availability falls on them as intermediaries in financial transactions. Given the critical role they play in ensuring the safety of financial assets, cybersecurity is essential to protect against threats such as data breaches, fraud, and ransomware attacks, which could have significant financial and reputational consequences.
- **Retail and e-commerce**
  Five companies were interviewed, which included online marketplaces, those that focus on special products, and logistics providers supporting e-commerce operations. These companies handle a significant volume of customer data, including personal information and payment details. They

also manage inventory, supply chain logistics, and customer order fulfilment. Given their heavy reliance on digital platforms to engage with customers and manage transactions, the companies in this sector are highly vulnerable to cyber threats such as phishing, malware, and data breaches. Particularly in busy sales seasons, effective cybersecurity policies are absolutely essential to guarantee client confidence, prevent identity theft, and preserve continuous services.

- **Manufacturing**

  Three manufacturing companies were interviewed. The interviewed companies operate in various industries, including consumer goods, automotive parts, and machine industry. These companies use interconnected systems, including Industrial Control Systems (ICS) and IoT-enabled devices, for production, quality control, and logistics management. The integration of these technologies in manufacturing has made manufacturing processes more efficient but has also increased the attack surface for cybercriminals. Unauthorised access to control systems could disrupt production schedules, compromise product quality, or expose proprietary data. Cybersecurity is critical in this sector to protect operational continuity, intellectual property, and supply chain integrity.

- **Mining**

  For this sector, two companies were interviewed. Their focus is on resource extraction and mineral processing. These companies have adopted digital systems to optimise mining operations, monitor equipment, and enhance safety. The reliance on technology for operational efficiency and remote monitoring makes mining companies targets for cyber-attacks aimed at disrupting operations or stealing proprietary data. In the mining sector, cybersecurity is particularly important to protect sensitive geological data, prevent operational disruptions, and ensure the safety of workers in hazardous environments. A successful cyber-attack could lead to operational

downtime, which is costly and potentially dangerous given how the industry is dependence on real-time data for safe operations.

The companies interviewed across these four sectors highlight the diversity in their operations and the shared importance of cybersecurity to protect their assets, sensitive data, and operational efficiency. Whether managing financial transactions, processing customer orders, manufacturing goods, or extracting resources, these companies are reliant on digital systems, making them vulnerable to cyber threats. Cybersecurity is therefore crucial for maintaining business continuity, customer trust, and overall resilience against potential attacks in each of these sectors.

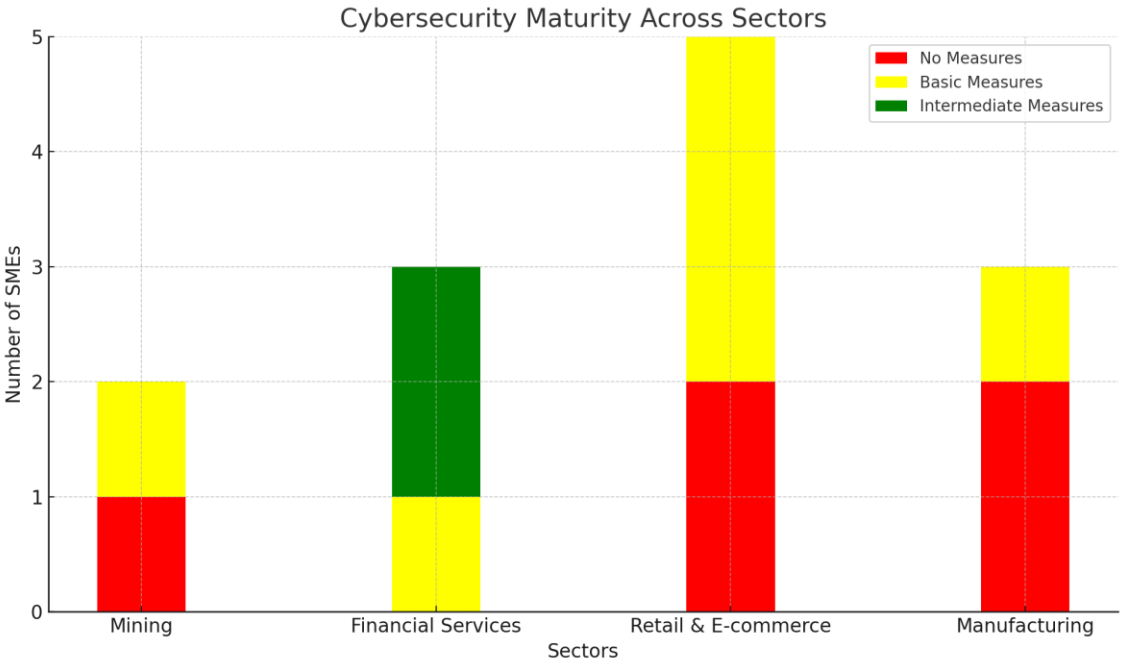


Figure 4-2: The cybersecurity maturity graph illustrates the varying levels of cybersecurity implementation across the four sectors analysed (Mining, Financial Services, Retail & e-commerce, and Manufacturing).

The data highlights a significant disparity, with sectors like Financial Services demonstrating higher levels of intermediate measures compared to others, such

as Mining and Manufacturing, which predominantly rely on basic or no measures. This disparity underscores the influence of sector-specific risks, regulatory pressures, and available resources. The findings reinforce the need for tailored strategies to address gaps in sectors lagging in cybersecurity maturity, aligning with the objective of the study to enhance SME resilience against cyber threats. The "no measure" category represents SMEs with no formal cybersecurity frameworks, leaving them highly vulnerable. "Basic measures" include fundamental protections like antivirus software and firewalls, offering minimal defense. "Intermediate measures" indicate a more structured approach with encryption, multifactor authentication, and periodic security assessments but still lacking advanced threat detection systems.

4.2.3 *Geographic Representation of Participating Companies*

Of the thirteen companies interviewed, seven are based in Gauteng, while the remaining six are spread across the country. Gauteng, as the economic hub of South Africa, hosts most of the SMEs, which makes this sample representative of the larger SME landscape in South Africa. The high concentration of SMEs in Gauteng reflects broader national trends, where the province is known for its high density of business activity, particularly in sectors such as financial services, retail and e-commerce, and manufacturing. This geographic distribution in the sample allows the study to capture cybersecurity practices and challenges faced by SMEs operating around the country.

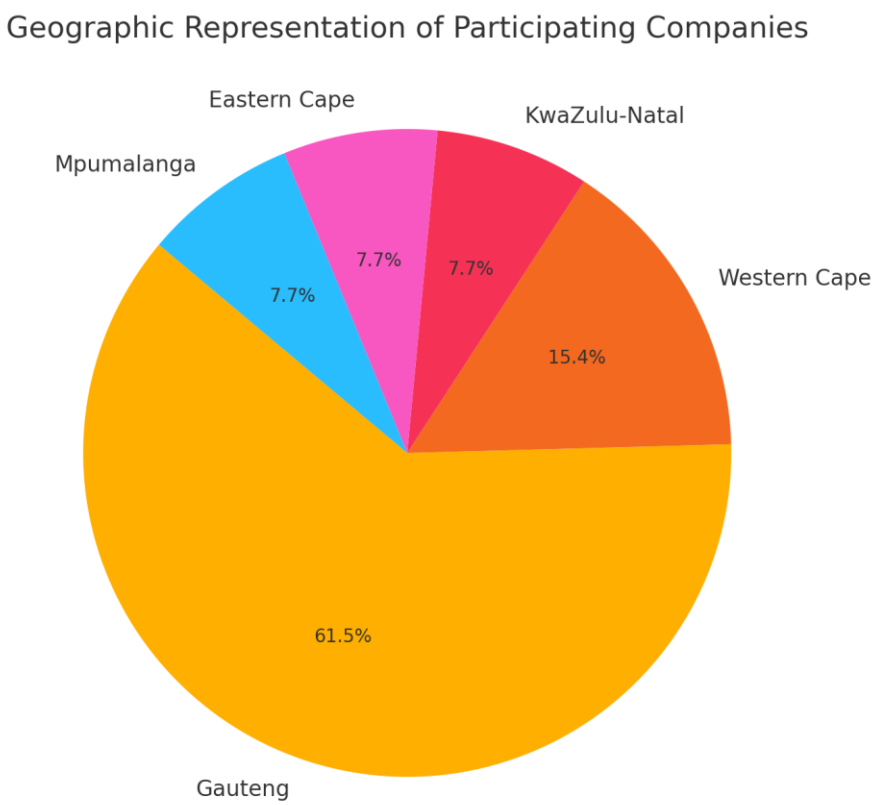


Figure 4-3: Graphical representation of SMEs per province.

4.3 Thematic Analysis

The thematic analysis was guided by the propositions presented in Chapter 2 (Table 2.1). Where relevant, themes are linked back to these propositions to evaluate theoretical consistency and uncover practical nuances.

To analyse the qualitative data collected from interviews, a thematic analysis approach was adopted using Atlas.ti. This was to facilitate the coding and organisation of data, allowing for the systematic identification of recurring patterns and themes.

The thematic analysis presented in this chapter is informed by the five theoretical propositions developed in Chapter 2, which are grounded in RBV, DOI, and TAM. These propositions served as an analytical lens through which to interpret and

organise the empirical data collected from the participating SMEs. While themes emerged inductively through coding, their interpretation is anchored in the propositions to ensure consistency with the study's theoretical framework. As such, key themes identified in the analysis are cross-referenced with the relevant propositions to establish theoretical alignment. This approach strengthens the interpretive depth of the findings and sets the foundation for discussion in Chapter 5.

The process began with the first round of open coding, where meaningful segments of data were assigned descriptive labels. These codes were iteratively refined and grouped into broader categories.

4.3.1 *Step 1: Codes*

Codes were created to represent key phrases, concepts from the research. A total of fifteen codes were generated, including but not limited to:

- **Financial Constraints**
- **Lack of Expertise**
- **Regulatory Pressures**
- **Basic Security Measures**
- **Advanced Security Measures**
- **Cybersecurity Awareness**
- **External Service Dependency**
- **Phishing Attacks**
- **Ransomware Incidents**
- **Data Breaches**
- **Network Monitoring**
- **Compliance Challenges**

- **Incident Response**
- **Budget Prioritisation**
- **Training Needs**

From these codes, key themes were derived, which form the structure of the subsequent sections of this chapter. These themes include the varying levels of cybersecurity implementation, challenges in adopting and maintaining measures, and the perceived effectiveness of existing systems.

The themes were then aligned with the research objectives, ensuring that the findings directly contribute to answering the key questions. The coding process provided a clear framework for organising the data, allowing for analysis of the cybersecurity landscape among SMEs in South Africa.

4.3.2 *Step 2 Develop the Themes*

Themes are broader categories that emerge from codes and will help connect analysis back to the research objectives and in chapter 5 we link them to the literature review. Based on the discussions in the chapters, here are the key themes:

a) Themes under Objective: Identifying Technical Cybersecurity Measures

In this section, we present the types of technical cybersecurity measures currently implemented by the participating SMEs across the different sectors. The focus is on the common types of cybersecurity solutions adopted, the technologies employed, and the general level of maturity of the cybersecurity infrastructure. This provides an understanding of how SMEs are responding to the evolving threat landscape and preparing their defences.

"We primarily use firewalls and endpoint security, but we still struggle with advanced threat detection," said Participant 5, highlighting a common limitation across multiple SMEs.

Of the thirteen companies interviewed, eight had some cybersecurity measures in place, while five had none. This difference draws attention to the varying degrees of cybersecurity readiness among SMEs in different fields. One participant pointed out, "We only have basic antivirus, nothing else beyond that. Though we are aware it is insufficient, we are not sure where to start." Conversely, Participant 11 from a company without any policies said, "We have not implemented any cybersecurity tools yet, mostly because we do not fully understand what we need or how to prioritise it."

The results of this research mirror the (World Economic Forum, 2025) report on supply chain interdependencies and AI-driven threats. Participants cited supply chain vulnerabilities as a significant concern, particularly in manufacturing which is reliant on third-party providers. Additionally, while AI's potential to enhance cybersecurity was acknowledged, none of the SMEs interviewed had assessed the security of AI tools, aligning with the report finding that only 37% of organisations globally have implemented processes to evaluate AI security(Forum, 2024).

The interviews revealed that most SMEs employ a basic set of security measures, such as firewalls, antivirus software, and encryption protocols, but the deployment of more advanced solutions like Intrusion Detection Systems (IDS) and Security Information and Event Management (SIEM) is less frequent.

- **Theme 1: Varying Levels of Cybersecurity Implementation**
  Participants highlighted differences in the deployment of cybersecurity measures:

    - Financial services SMEs generally had more advanced security measures, such as firewalls, encryption protocols, and endpoint protection software.
    - Retail and e-commerce SMEs often relied on basic measures that complied with minimum regulatory standards, like basic firewalls and anti-virus software.
    - Some manufacturing and mining SMEs lacked comprehensive cybersecurity frameworks, primarily due to limited resources and awareness.
- **Theme 2: Dependence on External Service Providers**
    - Many SMEs, especially in sectors like mining and retail, relied on third-party service providers for implementing and maintaining cybersecurity measures.

b) Themes under Objective: Challenges in Implementing Cybersecurity Measures

This section delves into the perceived effectiveness of the implemented cybersecurity measures, as reported by the participants. The focus here is to determine how well these measures are protecting SMEs from cyber threats and whether they provide sufficient defense against incidents such as ransomware, phishing, and data breaches. The effectiveness is also examined based on the participants satisfaction with the results of their current cybersecurity investments.

"We have managed to prevent a few phishing attempts, but I still feel that our systems are not robust enough to handle sophisticated attacks," expressed Participant 9, indicating a mixed perception of effectiveness.

Among the companies with cybersecurity measures, Participant 6 shared, "Our firewall has stopped several intrusion attempts, but we still feel vulnerable because we lack continuous monitoring." Conversely, Participant 12, whose company had no measures in place, said, "Without any cybersecurity tools, we are always worried about data breaches, and we know we are at high risk."

The analysis shows that while the majority of participants feel their cybersecurity measures are somewhat effective in mitigating low-level threats, they also express concerns about being inadequately prepared for more sophisticated attacks.

- **Theme 1: Financial Constraints**
    - Most participants cited budget limitations as a significant barrier to implementing advanced cybersecurity measures. The high cost of technology and expertise makes it difficult for SMEs to adopt comprehensive solutions.
- **Theme 2: Lack of Technical Expertise**
    - Respondents in all sectors, particularly those in retail and mining, mentioned the lack of in-house cybersecurity expertise as a challenge.
    - Some SMEs expressed a need for specialised knowledge to effectively configure and manage their cybersecurity systems.
- **Theme 3: Regulatory Compliance Pressures**
    - Financial services SMEs face strict regulatory requirements, such as POPIA, which necessitate higher standards of data protection. Meeting these requirements can be resource-intensive for smaller firms.

c) Themes under Objective: Evaluating the Effectiveness of Current Cybersecurity Measures

This section provides an overview of the challenges SMEs face in implementing effective cybersecurity measures. By understanding these challenges, we can contextualise why certain SMEs are more vulnerable and how these barriers affect their overall cybersecurity posture.

"Budget is always a problem. We cannot afford the latest security solutions, which leaves us exposed to threats" noted Participant 3, a sentiment echoed by other participants.

Financial constraints were cited as a significant barrier by most of the participants. As Participant 8 explained, "The cost of implementing even basic cybersecurity tools is too high for us right now." Another challenge mentioned was lack of knowledge and expertise. Participant seven said, "We do not have the technical skills in-house, and hiring experts is beyond our budget."

The interviews highlight financial limitations as one of the major barriers for SMEs, making it difficult for them to invest in more comprehensive cybersecurity solutions. A lack of skilled personnel to manage and implement these measures was also mentioned by some of the interviewed companies as a significant hindrance.

- **Theme 1: Mixed Perceptions of Effectiveness**
    - While some financial services SMEs felt confident about their cybersecurity posture, others in the same field, in retail and manufacturing acknowledged gaps in their protection against emerging threats.
- **Theme 2: Instances of Successful Mitigation**
    - One participant provided an example where firewall and intrusion detection systems successfully detected and mitigated threats,

such as phishing attempts. Two participants had example of the firewall detecting but they do not know what to do from there. So, there is measure in place to detect, which is just the basic.

- **Theme 3: Breaches and Lessons Learned**
    - Some SMEs, particularly in mining and retail, shared experiences of data breaches and highlighted the need for continuous monitoring and updates to their systems.

d) Linking the codes to the themes

Below is a graphical representation of how the themes mentioned link to the themes.

Figure 4-4: The above diagram is just to indicate how the themes link back to the codes.

4.4 Cybersecurity Documentation and Logs

During the interviews, participating SMEs were asked about their use and management of cybersecurity documentation and logs. While none of the SMEs provided documentation for review due to confidentiality concerns, discussions about logs revealed valuable insights. Only four SMEs with cybersecurity measures in place agreed to discuss their logs, and two of these companies shared their screens via Microsoft Teams to visually demonstrate the logs without sending the actual documents.

The logs discussed primarily included records of firewall activity, intrusion detection alerts, and endpoint security updates. Participants noted that these logs were instrumental in identifying potential threats but also highlighted gaps in their existing systems.

"We review our logs weekly, but even when we notice some anomalies, we cannot fully investigate due to limited resources," shared one participant. This underlines the reliance on basic monitoring systems, which lack the sophistication needed for proactive threat detection. Another participant, who demonstrated their logs, explained, "Our logs showed multiple phishing attempts, but we often only catch them after the fact, which is not ideal."

These discussions reinforced the narrative that existing measures were often inadequate. While logs provided evidence of attempted breaches, the lack of advanced monitoring and analysis tools left SMEs vulnerable to emerging threats. This finding ties back to the challenges highlighted in the literature review, which emphasises the importance of continuous monitoring and real-time threat detection as outlined in industry standards like the NIST Cybersecurity Framework

4.5 Participant Quotes and Insights

In addition to some of the quotes shared above, the table below highlights key quotes from the interviews, categorised according to the primary themes derived from the interview questions (Appendix A). These quotes provide a qualitative dimension to the findings, offering insights into participants real-world experiences, challenges, and perceptions regarding cybersecurity practices. By presenting direct voices from the field, this section strengthens the study's connection to practical realities and emphasises the diversity of perspectives across sectors.

The following table presents key quotes from participants, categorised by question heading, participant quotes, and sector. It captures the perspectives of SMEs on cybersecurity challenges, strategies, and regulatory compliance across different industries. By analysing these

responses, the study highlights recurring themes and sector-specific concerns, providing a deeper understanding of how SMEs perceive and implement cybersecurity measures.

Question Heading	**Participant Quote**	**Sector**
Existing Cybersecurity Measures	"We have antivirus software and firewalls, but they are not enough to handle the sophisticated threats today."	Retail & e-commerce
Existing Cybersecurity Measures	"Our systems are outdated; we don’t even have encryption protocols in place."	Retail & e-commerce
Challenges in Implementation	"Our biggest challenge is budget. We cannot afford advanced tools or hire specialists."	Manufacturing
Challenges in Implementation	"We lack the technical skills to manage even the basic cybersecurity tools we have."	Manufacturing
Regulatory Compliance	"Complying with POPIA is overwhelming for a small business like ours, both financially and operationally."	Financial Services
Regulatory Compliance	"GDPR compliance from third-party suppliers has added extra pressure on us."	Financial Services
Effectiveness of Current Measures	"Our firewalls have prevented a few attacks, but we still feel exposed to insider threats."	Manufacturing
Effectiveness of Current Measures	"We’ve caught phishing attempts through our endpoint security, but advanced threats remain a concern."	Retail & e-commerce
Technical Expertise	"We rely entirely on a third-party provider because we don’t have the skills to manage cybersecurity in-house."	Retail & e-commerce

Technical Expertise	"Training staff on cybersecurity is a constant struggle due to turnover and lack of interest."	Manufacturing
Incident Response Preparedness	"If we get hacked, I honestly don't know what the first step would be. We do not have a plan in place."	Mining
Incident Response Preparedness	"Our incident response plan is just a document. We have never tested it in a real scenario."	Mining
Adoption of Advanced Technologies	"AI-powered tools sound great, but they seem out of reach for us financially and technically."	Retail & e-commerce
Adoption of Advanced Technologies	"We've considered SIEM solutions, but the cost is a barrier we can't overcome right now."	Financial Services
Perception of Cyber Threats	"We know the risks are real, but cybersecurity feels like a luxury we can't afford right now."	Mining
Perception of Cyber Threats	"Cyber threats are always evolving. It feels like we are always a step behind."	Retail & e-commerce

Table 4-2: This table summarises participant responses across various cybersecurity themes, offering insights into sector-specific challenges and common trends in cybersecurity adoption among SMEs.

4.6 Summary of Findings

The findings presented in this chapter are aligned with the research objectives, providing insights into the current state of cybersecurity measures within South African SMEs, their effectiveness, and the challenges faced in implementation. The disparity in preparedness among SMEs ranging from those with advanced measures to those with none, addresses the first objective by identifying the spectrum of cybersecurity practices across sectors. The challenges highlighted,

such as financial constraints, lack of expertise, and regulatory compliance pressures, respond to the second objective, offering a deeper understanding of the barriers that hinder effective cybersecurity. Additionally, the analysis of the effectiveness of current measures, including instances of successful mitigation and vulnerabilities due to inadequate systems, fulfils the third objective by examining how existing solutions protect SMEs against cyber threats. This chapter sets the stage for discussing actionable strategies and best practices in subsequent sections, aiming to bridge the identified gaps and enhance cybersecurity resilience.

The data reveals that while some SMEs have made strides in adopting technical cybersecurity measures, significant gaps remain, especially in sectors with limited resources. Financial constraints, lack of expertise, and regulatory pressures are common challenges across sectors, influencing the overall effectiveness of cybersecurity strategies.

CHAPTER 5. DISCUSSION OF THE FINDINGS

5.1 Introduction

This chapter interprets the findings from the interviews in relation to the research objectives and literature. The analysis from Chapter 4, which highlighted both the technical cybersecurity measures implemented, and the challenges faced, provides the foundation for this discussion. By linking these findings to the literature discussed in Chapter 2, we gain a deeper understanding of the challenges and opportunities for enhancing cybersecurity resilience within the SME sector in South Africa. We then discuss how the results align or differ to the literature.

5.2 Discussion of Findings in Relation to Literature

The findings align with existing literature that emphasises the persistent struggles SMEs face in effectively implementing cybersecurity measures. Many SMEs still rely on traditional perimeter-based security strategies, which are insufficient in addressing the complex and evolving cyber threat landscape.

For example, (Amrin, 2014) emphasises that SMEs often perceive themselves as less attractive targets for cybercriminals compared to larger corporations. This misconception leads to a false sense of security, resulting in low prioritisation of cybersecurity investments. Similarly, (Manzoor et al., 2024) found that many SMEs operate with limited financial and technical resources, further reinforcing their reluctance to allocate budgets for advanced security systems. Their studies highlight that this underestimation of cyber threats often results in reactive approach rather than proactive security strategies, exposing SMEs to potential financial and reputational damages.

These findings align with the broader argument that SMEs lack of cybersecurity investment is not only a result of financial limitations but also of basic misinterpretation of risk exposure. As a result, this gap in awareness and investment perpetuates vulnerabilities, making SMEs an easy attractive target for cyberattacks. Addressing this issue requires awareness campaigns, tailored cybersecurity frameworks, and cost-effective security solutions to encourage SMEs to adopt a more proactive approach. This was reflected by one of the participants, who noted, "We primarily use firewalls and endpoint security, but we struggle with advanced threat detection."

The adoption of a zero-trust model, as highlighted by (Collard, 2025), could revolutionise how SMEs approach cybersecurity. Zero trust assumes no inherent trust within the network, requiring continuous verification of all users and devices. This approach directly addresses insider threats and challenges posed by remote work and cloud adoption. Participant 7 emphasised this challenge by stating, "We lack visibility into who accesses our network and for what purpose," a gap that zero-trust frameworks could help bridge through robust access controls and monitoring.

The importance of advanced incident response mechanisms was highlighted in this study, drawing parallels with case studies such as Fortinet's breach response. While Fortinet demonstrated the value of rapid containment, forensic analysis, and preventive measures, SMEs often lack the capacity to implement similar strategies. As Participant 3 admitted, "We do not have a response plan in place. If something happens, we are not sure where to start." This reflects findings by (Kariuki et al., 2023) and (Chingoriwo, 2022) which emphasise that SMEs are disproportionately affected by a lack of structured response protocols and skilled personnel.

This section interprets the study's findings through the lens of the five theoretical propositions outlined in Chapter 2, which are grounded in the Resource-Based View (RBV), the Diffusion of Innovations (DOI), and the Technology Acceptance Model (TAM). These propositions were developed to guide the analysis and ensure theoretical alignment between literature and the observed cybersecurity practices in South African SMEs. For instance, Proposition 1 (P1) posits that internal capabilities influence cybersecurity tool use. The findings strongly support this, revealing that SMEs with internal IT personnel or prior investments in IT infrastructure were more likely to adopt sophisticated tools such as SIEM systems and endpoint detection technologies. This validates the RBV framework, which emphasises that strategic resources and internal capabilities are essential enablers of technology adoption. However, the data also indicates that even resource-equipped SMEs encountered challenges in customising these tools to fit local needs and constraints. Similar alignments and divergences are discussed in relation to the remaining propositions highlighting how sectoral context, regulatory pressure, perceived complexity, and external support influence the adoption and effectiveness of cybersecurity measures.

5.2.1 *The Impact of Financial Constraints on Cybersecurity*

The findings confirm that limited financial resources hinder SMEs ability to implement robust cybersecurity measures. Eight of the companies interviewed had some measures in place, but they relied on basic, cost-effective solutions such as firewalls and antivirus software. Participant three highlighted that "Budget is always a problem. We cannot afford the latest security solutions, which leaves us exposed." This sentiment reflects the findings in the literature by (Alexander, 2021) and (UJ-TRCTI, 2022) , which emphasised that financial constraints prevent SMEs from adopting more advanced security technologies. The five companies without any measures in place echoed similar concerns about

affordability and access to funds. The study suggests that managed security services could provide a more cost-effective approach for SMEs to improve their cybersecurity, a solution that aligns with prior research suggesting shared services to overcome budget limitations.

In summary, the findings confirm that limited financial resources hinder SMEs ability to implement robust cybersecurity measures. This aligns with previous research that highlights budgetary constraints as a major barrier for SMEs globally. The study suggests that more cost-effective solutions, such as managed security services, could address some of these challenges.

5.2.2 *The Role of Expertise in Cybersecurity Implementation*

The study highlighted a recurring theme, which was ‘’the critical role of expertise in cybersecurity implementation’’. This finding aligns with (Chingoriwo, 2022) observation that cybersecurity frameworks often fail in contexts where end users lack adequate technical knowledge. In the context of SMEs, this gap is particularly pronounced, as many lack the in-house expertise required to configure and manage sophisticated cybersecurity systems. (Kariuki et al., 2023) further corroborated this, noting that small medium African enterprises are frequently targeted due to limited cybersecurity awareness and a lack of technical capacity to safeguard their digital operations. This lack of expertise leaves SMEs vulnerable to threats such as phishing and ransomware attacks.

Participants in this study echoed these sentiments. For example, Participant 7 stated, "We do not have anyone in-house who can help us understand the risks or set up proper defences," highlighting the dependency on external service providers. The reliance on outsourced expertise, while beneficial in some respects, also introduces vulnerabilities, such as limited oversight and the potential for misaligned priorities between SMEs and their vendors. These findings underscore

the urgent need for capacity-building initiatives tailored to SME contexts, such as practical training programs and affordable access to managed cybersecurity services. This concern was voiced by Participant 8, who noted that "Outsourcing cybersecurity is convenient, but it means we are always dependent on someone else to fix our problems." The need for in-house cybersecurity knowledge is highlighted by the literature as crucial for long-term resilience (Rawindaran et al., 2023).

In summary, the lack of specialised knowledge among SMEs is consistent with prior studies, which emphasise the need for skilled professionals in managing cybersecurity. Outsourcing to external providers appears to be a common approach, though it raises concerns about dependency and the adequacy of external support.

5.2.3 *Regulatory Pressures and Compliance Challenges*

The importance of regulatory compliance, particularly in sectors like financial services, was emphasised in the findings. Regulatory frameworks such as POPIA and GDPR act as both enablers and barriers for SMEs. While they push SMEs to adopt better data protection practices, they also impose financial and operational burdens that many find difficult to overcome. As Participant 6 remarked, "We must comply with POPIA, which means we need to have certain security standards, but it is costly and complex." This aligns with insights from (Ahmed & Nanath, 2021)and (Ncubukezi, 2023), who emphasise that while compliance fosters improved cybersecurity postures, it often creates challenges due to the limited financial and technical resources of SMEs. (Wolford) also shared same sentiments.

Further, (Yudhiyati & Putritama, 2021) highlight that SMEs in developing countries often struggle with awareness and understanding of

compliance requirements, which mirrors the findings of SMEs uneven knowledge of regulatory obligations. These challenges underline the critical need for targeted support from policymakers and industry stakeholders to help SMEs bridge the gap between compliance and practical implementation. Addressing these challenges is not only essential for the resilience of individual businesses but also for the broader digital economy that depends on their integration into global value chains.

In addition to the regulatory pressures, other challenges SMEs face in aligning their cybersecurity practices with emerging regulatory standards, is evolving cybersecurity standards. An example of that is upcoming FSCA's Joint Standard on Cybersecurity and Cyber Resilience, which is set to take effect in June 2025(ITWEB, 2024). This regulation, developed by the Financial Sector Conduct Authority (FSCA) in collaboration with the South African Reserve Bank (SARB), mandates robust governance structures, comprehensive cybersecurity strategies, and proactive measures like vulnerability assessments and penetration testing(ITWEB, 2024). While this represents a critical step in mitigating risks within the financial sector, it also amplifies the challenges for SMEs, especially those already constrained by financial and expertise gaps.

This aligns closely with the findings presented in Chapter 4, where several participants highlighted their struggles with implementing advanced cybersecurity measures. Participant nine remarked, "Our current systems are not robust enough to handle sophisticated threats," a sentiment echoed by others who expressed concerns about their capacity to comply with complex regulatory requirements. For SMEs with minimal or no cybersecurity measures, such mandates may appear unattainable without external support or significant resource allocation.

5.2.4 *The Role of Proactive Resilience*

The findings further reveal that many SMEs in the financial sector struggle to adopt proactive measures like penetration testing and cyber resilience assessments due to resource limitations.

This gap highlights the importance of partnerships with managed service providers (MSPs), which can enable SMEs to stay ahead of evolving cyber threats. MSPs offer a range of security services, including continuous network monitoring, threat detection and response, firewall management, endpoint protection, and compliance support. These services are particularly valuable to SMEs, as they alleviate the burden of hiring in-house cybersecurity experts, a challenge many SMEs face due to budget constraints and skills shortages. By leveraging MSPs, SMEs can access enterprise-level security solutions at a fraction of the cost of building an in-house cybersecurity team.

Furthermore, MSPs provide scalability and flexibility, allowing SMEs to tailor security solutions to their needs as they grow. Proactive threat management is another key advantage, as MSPs use advanced security tools, AI-driven analytics, and 24/7 monitoring to detect and mitigate cyber threats before they cause considerable damage.

However, while MSPs offer critical security enhancements, there are potential downsides that SMEs must consider. Vendor lock-in can be a concern, as SMEs may become dependent on a single provider, making it difficult to transition to another vendor without significant disruptions. Cost can also be a limiting factor, especially for small businesses with minimal IT budgets, as MSP services may still represent a significant expense. Additionally, entrusting sensitive business data to a third party introduces security and privacy risks, as MSPs have access to critical systems and confidential information. Poorly managed service agreements or insufficient oversight could lead to compliance violations, data breaches, or insider threats from MSP personnel.

Despite these challenges, the benefits of partnering with an MSP often outweigh the risks, especially when SMEs implement due diligence in how they do vendor selection, negotiate clear service level agreements (SLAs), and maintain internal oversight of outsourced security functions. By doing so, SMEs can effectively bridge their cybersecurity gaps while minimising potential downsides, ensuring robust protection without overstretching their internal resources.

These services not only align with regulatory requirements but also empower SMEs to build stronger defences against an increasingly complex cyber threat landscape.

Ultimately, the FSCA's Joint Standard represents both a challenge and an opportunity for financial SMEs. While the regulatory requirements may strain already limited resources, they also incentivise the adoption of advanced, AI-driven solutions that can significantly enhance cybersecurity resilience.

In Summary, the emphasis on compliance with data protection laws, particularly in financial services, underscores the importance of regulatory frameworks in shaping cybersecurity practices. While regulations like POPIA can push SMEs to adopt better data protection measures, they also impose additional financial and operational burdens.

5.3 Implications for SMEs and Cybersecurity Practices

The findings of this study carry significant implications for how SMEs approach cybersecurity. The challenges identified—such as financial constraints, lack of expertise, and regulatory compliance pressures—underscore the complex landscape in which SMEs must operate. The study highlights how sector-specific needs shape cybersecurity priorities, with financial services firms requiring

stringent security measures due to regulatory obligations, while e-commerce businesses focus on securing customer transactions.

The study has several implications for SMEs and their approach to cybersecurity. Firstly, there is a clear need for tailored cybersecurity strategies that consider the specific challenges faced by each sector. For example, companies in financial services need more robust solutions due to the sensitive nature of the data they handle, whereas e-commerce companies may benefit more from solutions aimed at protecting customer data during transactions.

The study also suggests that financial incentives or support from industry bodies could play a critical role in encouraging the broader adoption of cybersecurity measures among SMEs. Participant two suggested, "If there were grants or subsidies to help us implement these systems, it would make a big difference." This aligns with recommendations from previous studies that emphasise the role of financial support in enabling SMEs to overcome barriers to cybersecurity implementation (UJ-TRCTI, 2022).

Moreover, building internal capacity through training and awareness could help reduce reliance on external providers. Many participants highlighted the importance of employee awareness in preventing incidents like phishing attacks. As Participant 9 noted, "Our employees need more training on identifying suspicious emails, it is often human error that leads to problems." The literature also underscores the role of continuous training in enhancing cybersecurity resilience, especially in environments where resources are constrained (Alexander, 2021).

The findings of this study confirm the critical issues highlighted in the *Global Cybersecurity Outlook 2025(World Economic Forum, 2025)*, particularly the deepening divide between large organisations and SMEs regarding cybersecurity readiness. Regulatory fragmentation emerged as a recurring theme in both the global report and this study, with SMEs struggling to navigate compliance with laws like POPIA while meeting operational demands. The

report calls for a shift from cybersecurity to enhanced cyber resilience resonates with the need for SMEs to prioritise proactive risk management strategies, as observed in this research.

In Summary,

- The study highlights the need for tailored cybersecurity strategies that consider the specific challenges of each sector.
- Financial incentives or support from industry bodies could encourage broader adoption of cybersecurity measures among SMEs.
- Building internal capacity through training and awareness could help reduce reliance on external providers.

5.4 Linking Cybersecurity Measures to Industry Standards

Although eight of the SMEs included in the study had implemented some form of cybersecurity measures, a deeper analysis against established industry standards reveals significant inadequacies. Standards such as the NIST Cybersecurity Framework, ISO/IEC 27001, and local compliance requirements like the FSCA Cyber Resilience Standards highlight the critical need for robust and proactive cybersecurity practices.

As noted in Participant 5's feedback, "We primarily use firewalls and endpoint security, but we struggle with advanced threat detection," a sentiment echoed by other SMEs across sectors. This points to a reliance on basic measures without the layered defences emphasised in industry standards. For example, industry guidelines advocate for continuous network monitoring, incident response planning, and vulnerability assessment, which are practices often missing among the SMEs surveyed.

The five SMEs with no measures in place, represented by Participant 12's statement, "We are aware of our vulnerabilities but do not know how to start addressing them," exemplify the gap between awareness and action. Even among SMEs with basic measures, compliance with standards such as the FSCA's Joint Standard requires more than endpoint protection and antivirus software; it mandates stringent identity and access management protocols, regular penetration testing, and comprehensive governance structures.

This finding underscores the gap between current practices and the industry's evolving demands. As seen in the literature, for example (Varachia, 2022) stated that compliance with these standards not only minimises risk but also enhances organisational resilience and customer trust. SMEs failing to align with these standards risk operational disruptions, financial losses, and reputational damage, especially in sectors like financial services where regulatory oversight is stringent.

5.5 Addressing the Research Objectives

The findings of this study directly address the research objectives by providing insights into how each objective was met:

Research Objective 1: Assess the Current State of Technical Cybersecurity Measures in South African SMEs

- The study revealed significant variations in the implementation of cybersecurity measures among SMEs. Out of the thirteen companies interviewed, eight had some form of cybersecurity in place, while five had none. The eight companies with measures primarily relied on basic tools such as firewalls, antivirus software, and limited encryption protocols. Despite these efforts, they lacked advanced tools like intrusion detection systems (IDS) and security information and event management (SIEM) systems. Participant five noted, "We primarily use firewalls and endpoint security, but we

still struggle with advanced threat detection," highlighting gaps in advanced security solutions. This finding aligns with (Erdogan et al., 2023), who identified resource constraints as a major barrier to comprehensive cybersecurity implementation among SMEs.

Research Objective 2: Evaluate the Effectiveness of Current Cybersecurity Measures in Mitigating Threats

- The effectiveness of existing cybersecurity measures varied significantly. Companies with basic measures managed to prevent common threats, such as phishing attacks. Participant nine stated, "We have managed to prevent a few phishing attempts, but I still feel that our systems are not robust enough to handle sophisticated attacks." This highlights the partial effectiveness of basic measures in mitigating low-level threats. However, companies without any measures were highly vulnerable to attacks, exposing their operations to significant risk. This observation aligns with (Naude et al., 2023), who emphasised the importance of even basic cybersecurity measures as a foundation for more advanced defences.

Research Objective 3: Identify Challenges Faced in Implementing and Maintaining Cybersecurity Strategies

- The study uncovered several challenges impeding the implementation of effective cybersecurity strategies. Companies without measures cited financial constraints and a lack of knowledge as primary obstacles. Participant eleven remarked, "We have not implemented any cybersecurity tools yet, mostly because we do not fully understand what we need or how to prioritise it." This finding underscores the importance of accessible information and resources for SMEs, echoing (Kariuki et al., 2023) who stressed the need for greater awareness and education within the sector.

Additionally, companies with existing measures identified challenges such as limited budgets for advanced tools and difficulties maintaining up-to-date security protocols.

5.6 Comparative Analysis of Interview and Literature Findings

In Chapter 2, a diagram illustrated key themes emerging from the literature. Below, a new diagram presents the key themes identified from the interviews, followed by a combined version that integrates both literature and interview findings.

Some of the themes uniquely observed in the literature include "Long-term Strategic Planning" and "Ethical Considerations in AI Use," which did not emerge from the interviews. Conversely, certain themes derived from interviews highlight practical challenges faced by SMEs that were less emphasised in literature. These interview-based themes warrant further exploration in future research.

The following diagrams represent these key themes in a graphical format, providing insights into how academic discussions and real-world SME experiences align and diverge.

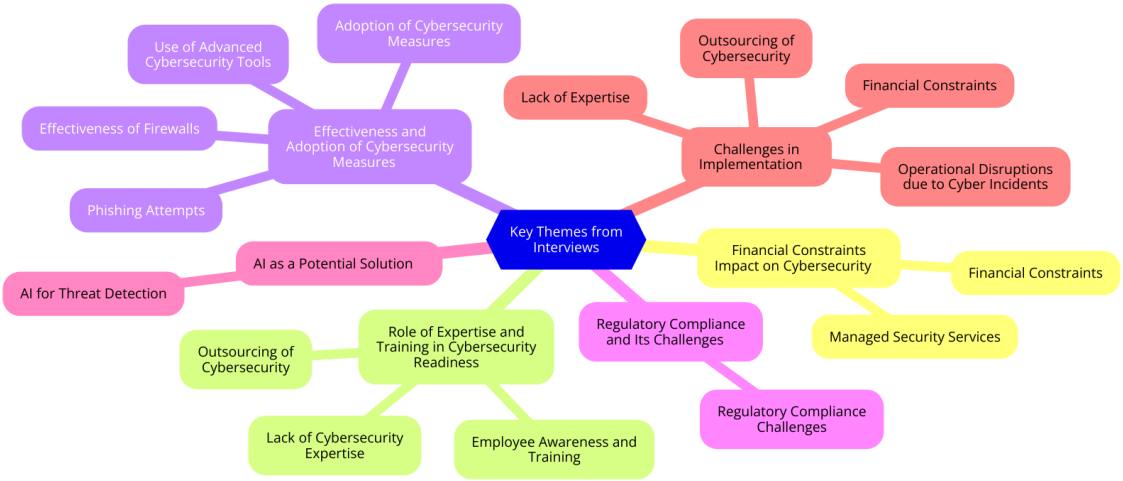


Figure 5-1: Above is a graphical representation of key themes from interviews.

Below is combination of the Key Themes from literature and interviews.

Figure 5-2: The combined diagram highlights shared themes that both interviews and literature had.

In addition to the above, the below table looked at the challenges versus the responses from the different sectors.

Challenge	**Financial Services**	**Retail & E-commerce**	**Manufacturing**	**Mining**
Cost of advanced tools	Use MSSPs	Cloud tools	Basic tools only	Outsource to MSPs

Lack of internal expertise	Hire in-house experts	External consultants	Minimal IT staff	Mixed expertise
Compliance with POPIA	Strong compliance	Partial compliance	Limited compliance	Moderate compliance
Lack of threat awareness	High awareness	Moderate awareness	Low awareness	Low to moderate awareness

Table 5-1: Cybersecurity Challenges vs. Responses by Sector

5.7 Narrative Analysis of Cybersecurity Maturity

In chapter 4 (**Figure 4-2)**, we presented a diagram for cybersecurity maturity across sectors, below is further analysis and linking it to the literature.

5.7.1 *Pattern Analysis*

The cybersecurity maturity table and visualisations highlight significant disparities across the sectors examined. Financial services SMEs demonstrate a relatively higher inclination toward intermediate measures, driven by regulatory pressures such as the POPIA and sector-specific regulation. This aligns with the literature that underscores the role of regulations in fostering improved cybersecurity practices (Wolford).

However, there is a notable pattern suggesting that some SMEs may be focusing on compliance rather than actual security improvements. Participant 6 reflected this concern, stating: “Complying with POPIA means meeting certain security standards, but the costs and complexities are immense.” This indicates that

regulatory compliance may be driving surface-level measures rather than comprehensive security strategies.

In contrast, sectors like mining and manufacturing predominantly exhibit basic or non-existent cybersecurity measures. The lack of regulatory pressures and the perception of cybersecurity as a non-priority for operational processes may contribute to these gaps. Participant 3 from a manufacturing SME commented: “Cybersecurity is something we know we need, but it always gets deprioritised because we focus on production.” This mirrors findings in the literature, which note that SMEs in less regulated sectors often lag in cybersecurity implementation (Chingoriwo, 2022).

5.7.2 *Insights*

These findings echo prior research emphasising the dual role of regulatory frameworks as both a driver and a burden for SMEs (Ncubukezi, 2023). While regulations like POPIA push financial SMEs toward better practices, the same frameworks create financial and operational burdens for resource-limited organisations(Alexander, 2021). The need for cost-effective solutions, such as AI-powered monitoring tools, emerges as a recurring theme. As Participant 8 observed: “AI-driven tools could help us manage security more effectively, but the upfront costs and technical know-how are out of reach.”

For SMEs in mining and manufacturing, targeted interventions are necessary to bridge the gap. Government incentives and partnerships with managed service providers can alleviate financial and technical barriers, enabling these sectors to adopt at least minimum-security standards.

These sectoral disparities align with findings from the (World Economic Forum, 2025) which identified regulatory fragmentation, financial constraints, and workforce challenges as key barriers to cybersecurity maturity. Additionally, studies by (Kariuki et al., 2023) and (Chingoriwo, 2022) emphasise that SMEs

often face decision paralysis due to the complexity of cybersecurity technologies, further delaying adoption.

5.8 Theoretical Reflections

The findings of this study were analysed considering the theoretical frameworks presented in Chapter 3, including the Technology Acceptance Model (TAM), Resource-Based View (RBV), and Diffusion of Innovations Theory. These theories provided a foundation for understanding SMEs adoption and implementation of cybersecurity measures.

5.8.1 *Alignment with Theoretical Expectations*

The study largely aligns with TAM's premise that perceived usefulness and ease of use drive technology adoption. SMEs that implemented basic cybersecurity measures often cited ease of deployment and immediate benefits, such as endpoint security and firewalls. As Participant 3 noted, "We chose a solution that our team could understand and manage without needing external expertise." This supports the TAM principle that ease of use is critical for adoption in resource-constrained environments.

Similarly, the Resource-Based View (RBV) is validated through both participant insights and literature findings. SMEs with stronger financial resources and internal expertise demonstrated a greater capacity to adopt comprehensive cybersecurity measures. For example, one participant from a financial services SME stated, “Having an in-house IT specialist allowed us to implement some security measures without relying on costly consultants.” This aligns with RBV's assertion that internal resources such as technical skills and financial capacity are critical for building competitive advantage. Additionally, (Chingoriwo, 2022)

reinforces that resource-rich SMEs are more likely to implement layered security measures, further validating the RBV framework..

5.8.2 *Divergence from Theoretical Expectations*

However, not all findings aligned with theoretical expectations. For instance, the Diffusion of Innovations Theory states that awareness, and perceived benefits should accelerate adoption. Despite high awareness of cybersecurity risks, some SMEs, particularly in retail and e-commerce, failed to act. As Participant 9 explained, "We understand the risks, but the costs and complexity are overwhelming." This divergence suggests that financial and resource constraints may override innovation diffusion in SMEs, requiring a nuanced understanding of barriers.

Alternative theoretical perspectives, such as Behavioural Economics, may help explain these findings more effectively. Behavioural Economics examines how psychological factors influence decision-making, especially under conditions of uncertainty or limited information(Good, 2019).

In this context, SMEs may experience two key behaviours:

- Risk Aversion - This means they tend to avoid actions that feel too risky, such as investing in cybersecurity, because they fear losing money without guaranteed returns. For example, the high upfront costs of security tools may seem too risky if they are unsure the tools will prevent future attacks.
- Decision Paralysis - This happens when SMEs feel overwhelmed by complex choices and uncertain outcomes, causing them to delay or avoid making decisions altogether. The technical complexity of cybersecurity solutions, combined with financial pressure, can lead to inaction.

These behaviours stem from financial pressures and uncertainty about whether the return on investment (ROI) from cybersecurity measures will justify the cost. In other words, SMEs may hesitate to act because they fear spending money on solutions that they do not fully understand or believe they may not need until it is too late.

By considering these behavioural factors, we can better understand why some SMEs fail to invest in cybersecurity, even when they acknowledge the risks of inaction.

The following diagram visually links the five propositions developed in Chapter 2 to the corresponding empirical findings presented in Chapter 4. This visual representation aids in demonstrating the consistency between theoretical expectations and observed cybersecurity practices in South African SMEs.

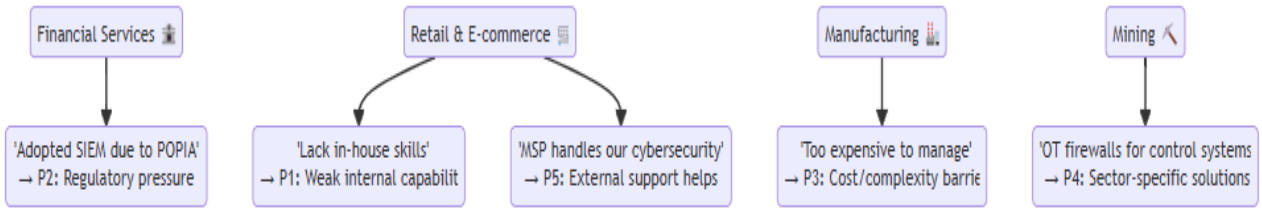


Figure 5-3: Visual Link Between Theoretical Propositions and Empirical Findings

This diagram illustrates the relationship between the five theoretical propositions and the key findings of the study. It demonstrates how the theoretical frameworks of RBV, DOI, and TAM were reflected in the empirical data.

5.9 Chapter Conclusion

Concluding chapter 5, the findings of this study provide critical insights into the challenges SMEs face in implementing and sustaining cybersecurity measures. Three key barriers; financial constraints, lack of expertise, and regulatory

compliance pressures interact to create a complex cybersecurity landscape for SMEs.

- Financial Constraints- Limited budgets often prevent SMEs from investing in advanced cybersecurity tools or hiring skilled personnel. This scarcity of resources forces SMEs to prioritise short-term operational needs over long-term security investments.
- Lack of Expertise- Without internal technical knowledge, SMEs struggle to choose, implement, and maintain appropriate security solutions. This gap increases their reliance on third-party providers, which may introduce additional costs or risks.
- Regulatory Compliance Pressures- Compliance requirements, such as POPIA, impose security standards that SMEs must meet to avoid penalties. However, meeting these standards often requires costly security tools and technical expertise—both of which may be out of reach for resource-constrained SMEs.

The interaction between these factors exacerbates the cybersecurity challenges for SMEs. For example, regulatory demands create a sense of urgency, but without financial resources and expertise, SMEs may adopt minimal, compliance-focused measures rather than comprehensive security strategies. This reactive approach can leave critical vulnerabilities unaddressed. Additionally, limited expertise can lead to poor decision-making, causing SMEs to overspend on ineffective solutions or face fines for non-compliance.

Overall Findings and Industry Context

- Analysis by (Cobos, 2024) reveals that developing countries account for 30% of publicly disclosed cyber incidents, with SMEs and public administration being particularly targeted. This trend mirrors the vulnerabilities observed among South African SMEs,

where limited resources and increasing digital adoption heighten exposure to cyber risks.

- The findings indicate that while some SMEs have taken initial steps toward implementing cybersecurity measures, there is still some gaps. Financial constraints, lack of expertise, and regulatory pressures continue to slow down progress. Addressing these issues requires a multi-faceted approach, including financial support, increased awareness campaigns, and industry-specific cybersecurity frameworks tailored to the needs of SMEs.

These findings align with research that was done before, which highlights the persistent struggles of small and medium-sized enterprises in balancing cybersecurity needs with resource limitations. Addressing these intertwined challenges requires tailored support, such as affordable security solutions, practical guidance on regulatory compliance, and skills development programs to empower SMEs in securing their operations effectively.

The discussion in this chapter linked the study's findings to existing literature, reinforcing that while SMEs recognise the importance of cybersecurity, many are unable to implement comprehensive solutions due to financial and technical limitations. The adoption of basic cybersecurity measures, such as firewalls and antivirus software, reflects the resource constraints that SMEs experience, with only a few organisations progressing toward intermediate or advanced security frameworks. This supports the Technology Acceptance Model (TAM), which suggests that perceived ease of use and usefulness significantly impact cybersecurity adoption in SMEs.

Additionally, regulatory compliance was found to be both a driver and a barrier to cybersecurity adoption. While frameworks such as POPIA and GDPR push SMEs to improve security standards, they also impose additional financial and operational burdens.

The study highlights the urgent need for specific policy interventions, including:

- Subsidies or tax incentives for SMEs investing in cybersecurity tools and services.
- Public-private partnerships to provide affordable cybersecurity training programs.
- Sector-specific regulatory frameworks that are adaptable to SMEs resource limitations.
- Government-backed certification programs that help SMEs meet compliance standards without excessive costs.

Additionally, industry support is essential, such as collaborative threat intelligence platforms tailored for SMEs and vendor-neutral advisory services to help SMEs make informed cybersecurity decisions. Financial incentives, such as low-interest loans or grants, can enable SMEs to adopt robust security measures without compromising their cash flow. A key implication of these findings is the growing dependency on external cybersecurity service providers due to the lack of in-house expertise. While outsourcing provides SMEs with access to advanced cybersecurity solutions, it also creates new vulnerabilities related to vendor dependency, data privacy risks, and potential misalignment with business objectives. This raises important considerations for balancing external support with internal capacity-building efforts.

The findings point to the need for tailored cybersecurity strategies that account for the unique constraints and priorities of different SME sectors. The financial services sector, for instance, faces stringent compliance obligations, necessitating advanced security solutions, while e-commerce SMEs prioritise securing customer transactions. Understanding these sector-specific cybersecurity needs is critical for designing effective, scalable, and sustainable security frameworks.

In summary, this study contributes to the broader discussion on SME cybersecurity resilience, reaffirming the necessity of cost-effective security solutions, targeted regulatory support, and continuous cybersecurity education. While SMEs may struggle to adopt enterprise-grade security frameworks, incremental improvement such as managed security services, employee training, and risk-based security models can enhance their cybersecurity posture and reduce exposure to emerging threats. These insights will be further expanded in the recommendations and concluding chapter that follows.

CHAPTER 6. CONCLUSIONS & RECOMMENDATIONS

6.1 Introduction

This chapter concludes the research and presents recommendations for SMEs and policymakers to enhance cybersecurity resilience. It also outlines the study's limitations and proposes directions for future research. The chapter highlights several potential solutions to address SMEs cybersecurity challenges including artificial intelligence (AI), managed cybersecurity services, employee training, and regulatory simplifications to tackle financial constraints, expertise gaps, and compliance pressures.

While AI-powered cybersecurity tools offer valuable solutions such as automated threat detection and continuous monitoring, other non-AI-based approaches are equally critical. Managed cybersecurity services help SMEs access expert security capabilities without the high costs of building in-house teams. Additionally, employee training programs strengthen internal capacity, reducing human errors that often lead to breaches. Finally, policy interventions, such as simplified compliance processes and financial incentives, can alleviate regulatory burdens and enable broader adoption of cybersecurity measures.

This approach encompassing technological innovation, capacity building, and regulatory support provides a comprehensive pathway for SMEs to enhance their cybersecurity resilience.

6.2 Contributions

Theoretical Contribution

The research extends the application of three theoretical frameworks, RBV, DOI, and TAM to the context of cybersecurity implementation among South African SMEs. By linking empirical findings to propositions grounded in these theories, the study confirmed and enriched existing perspectives on how internal capabilities, innovation diffusion, and perceived technology usability shape cybersecurity practices in resource-constrained environments. The proposition-driven analysis strengthens the theoretical grounding of SME cybersecurity literature.

Methodological Contribution

Methodologically, the study used a generic qualitative approach rooted in interpretivism, drawing on both semi-structured interviews and document analysis to examine cybersecurity practices in four SME sectors. This methodological triangulation enhances the reliability of the findings and provides a replicable approach for future research exploring technology adoption in SMEs. Moreover, the use of formal propositions to guide the thematic analysis demonstrated a structured way to align qualitative data with theoretical expectations.

Contextual Contribution

The study provided a contextual contribution by focusing specifically on SMEs in the South African market, a sector underrepresented in global cybersecurity research. The findings highlighted how regulatory pressure from POPIA, sector-specific risk exposure, and limited internal capabilities influence cybersecurity behaviours. Particularly, insights from the manufacturing and mining sectors offer nuanced understanding of how less-digitally mature SMEs respond to cybersecurity threats. These context-driven findings provide valuable guidance

for policymakers, support organisations, and solution providers operating in similar emerging market environments.

6.3 Summary of Key Findings

The study found that while some SMEs have implemented advanced cybersecurity measures, there is still a high number that still rely on basic or no protection, leaving them vulnerable to cyber threats. Financial constraints and lack of expertise emerged as major barriers to effective cybersecurity implementation, which is consistent with the existing literature. Regulatory pressures were another challenge, particularly in the financial services sector, which further complicate the adoption of robust cybersecurity measures.

Geographically, the study found that SMEs in Gauteng which is the economic hub of South Africa, were better represented in terms of basic technical cybersecurity measures compared to those in other provinces. This regional variation highlights the need for targeted interventions to support SMEs in more underserved areas.

6.4 Recommendations

6.4.1 *For SMEs*

- **Adopt Cost-Effective Cybersecurity Measures**

  SMEs should consider adopting managed cybersecurity services and open-source tools to enhance their protection without incurring significant financial burden. Managed security services provide an affordable way to access professional security monitoring and incident response, which is crucial given the limited internal resources that many SMEs face. The Fortinet incident mentioned in previous chapters illustrates the value of proactive measures such as enhanced monitoring, threat detection, and

engaging external cybersecurity experts(Fortinet, 2024). While SMEs often lack the resources to implement such advanced strategies independently, partnering with security providers help adopt proactive measures.

- **Incorporate Artificial Intelligence for Cybersecurity**

  SMEs should leverage AI-powered cybersecurity tools to actively monitor network traffic, identify unusual patterns, and detect potential breaches. AI can serve as an effective supplement to limited human resources, providing 24/7 monitoring and alerting SMEs to suspicious activities. As highlighted in the study, many SMEs lack the technical expertise to manage complex systems. AI can help fill this gap by automating threat detection, reducing false positives, and ensuring that incidents are flagged promptly.

  However, the adoption of AI must be done responsibly and with full awareness of its capabilities and limitations. SMEs should understand that while AI enhances detection and response capabilities, it is not a standalone solution. Clear guidelines on AI implementation, regular audits for algorithmic accuracy, and proper staff training on AI-driven tools are essential. Responsible use of AI also includes addressing ethical concerns, such as data privacy and bias in automated decision-making processes.

  By integrating AI with a well-rounded cybersecurity strategy, including human oversight and continuous evaluation, SMEs can maximise its benefits while mitigating potential risks. The integration of AI-driven solutions, such as managed detection and response, continuous vulnerability management, and real-time network monitoring, offers a promising pathway for SMEs to address these challenges. As discussed in this study, many SMEs lack internal capacity for ongoing monitoring and advanced threat detection. AI-enhanced services, such as those offered

by managed service providers, can fill this gap by automating incident detection, providing continuous compliance support, and facilitating proactive risk management. For example, one provider offers Cyber Resilience Assessment which helps businesses evaluate their readiness against industry standards like NIST and CIS, a need explicitly mentioned by Participant 7, who acknowledged their company limited internal capabilities.

The FSCA's emphasis on ongoing assessments and robust governance resonates with the broader recommendation for SMEs to adopt AI-driven resilience strategies, as proposed in Chapter 6. By leveraging AI for network monitoring, SMEs can address their limited technical expertise and financial constraints while aligning with regulatory expectations.

- **Invest in Training Programs**

  Building internal capacity through employee training programs is crucial to reduce dependence on external providers and minimise the risk of human error. Training employees to identify phishing attempts and understand the basics of cybersecurity can significantly enhance the overall cybersecurity posture of the organisation. As Participant 9 noted, "Our employees need more training on identifying suspicious emails, it is often human error that leads to problems."

- **Sector-Specific Cybersecurity Recommendations**

  Different sectors face unique cybersecurity threats and operational challenges, which necessitate tailored security measures. Factors such as regulatory requirements, data sensitivity, and the nature of digital operations influence the security needs of each industry. A one-size-fits-all approach is ineffective, as the risks faced by financial services providers differ significantly from those in manufacturing or mining.

Therefore, the following recommendations address sector-specific needs while aligning with industry best practices.

1. Financial Services - Strengthen compliance through AI-powered threat detection tools that streamline regulatory reporting and incident response.
2. Retail and e-commerce - Focus on endpoint security and payment fraud detection solutions tailored to customer data protection.
3. Manufacturing - Introduce scalable, low-cost solutions such as automated firewalls and intrusion detection systems to safeguard operational technology (OT).
4. Mining - Prioritise basic measures like encryption and periodic vulnerability assessments to protect sensitive operational data.

Picture representation of some of the recommendations for SMEs by sector below. Figure 6-1.

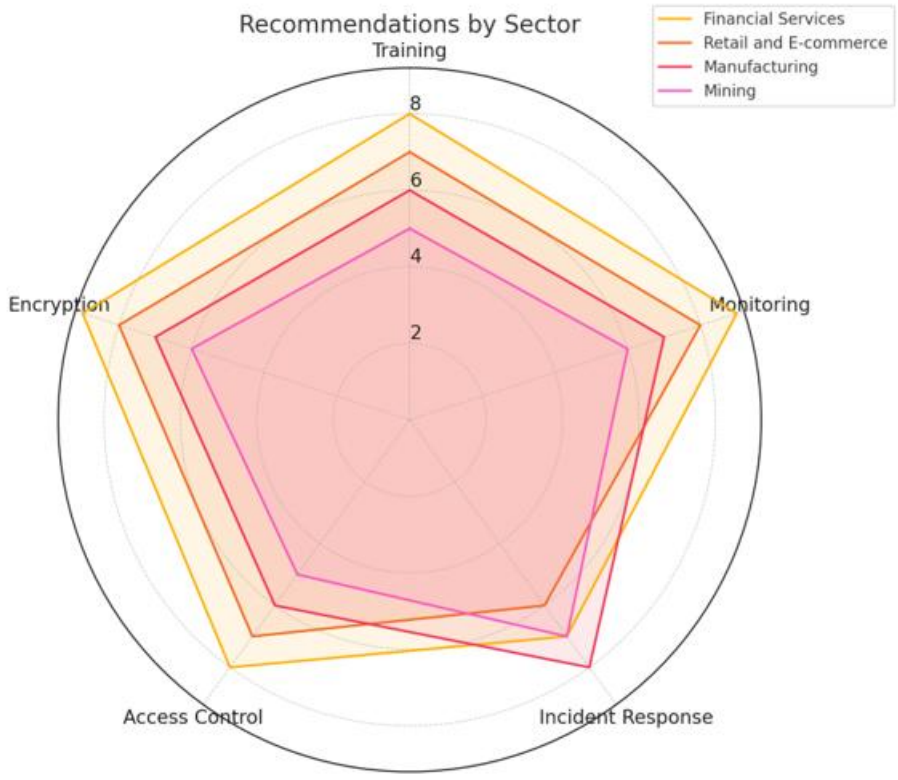


Figure 6-1: Recommendations for SMEs across sectors, including financial services, retail and e-commerce, manufacturing, and mining.

The diagram presents tailored cybersecurity recommendations for SMEs across sectors, including financial services, retail and e-commerce, manufacturing, and mining. These recommendations address both sector-specific needs and overarching cybersecurity priorities. Key measures include encryption protocols to safeguard sensitive data, continuous monitoring to detect and respond to threats in real-time, incident response plans to mitigate the impact of cyber incidents, and access control mechanisms to ensure that only authorised personnel can access critical systems.

Training initiatives are also highlighted, even though the focus of the paper is on technical measures. This inclusion is based on the recognition that technical systems can only be effective if employees have the necessary awareness and skills to use them properly. For instance, proper use of encryption and access control requires employees to understand their importance and follow established procedures. Training ensures that human errors, such as falling victim to phishing attacks or misconfiguring systems, do not undermine the effectiveness of technical cybersecurity measures.

The numbers in the diagram illustrate the progression and prioritisation of these recommendations. For example, encryption and access control are foundational measures for all sectors, while continuous monitoring and incident response plans are progressively implemented as resources and technical maturity improve. This structure reflects a practical roadmap for SMEs, helping them address the evolving cybersecurity threat landscape in a cost-effective manner.

6.4.2 *Recommendations For Policymakers*

Provide Financial Support and Incentives

- Policymakers should provide subsidies or financial incentives for SMEs to adopt advanced cybersecurity measures. Sectors like mining and retail, which tend to lag in cybersecurity adoption, could particularly benefit from such support. Financial incentives would help bridge the gap between basic protections and the more sophisticated solutions needed to safeguard against advanced threats.
- Additionally, policymakers should engage with the private sector to foster collaboration and resource-sharing initiatives. By partnering with technology providers and managed service providers, they can offer discounted cybersecurity solutions or services to SMEs. Such public-private partnerships would not only reduce costs for SMEs but also strengthen the overall cybersecurity posture of the country.

Encourage the Adoption of AI Technologies:

- Policymakers should encourage SMEs to adopt AI-based cybersecurity technologies by providing grants or facilitating partnerships with technology providers. AI has the potential to transform SME cybersecurity by offering cost-effective, scalable solutions that continuously monitor and respond to threats, which aligns with findings from the literature(Rawindaran et al., 2023) .

- Building on the insights from(World Economic Forum, 2025), this study recommends a stronger focus on collaboration and resource-sharing within SME ecosystems to address cybersecurity challenges. Supply chain risks, as highlighted in the report, can be mitigated through shared cyber resilience frameworks and cross-sector partnerships. Furthermore, integrating AI-powered solutions for real-time threat detection and risk assessment can enhance SMEs cybersecurity posture, provided adequate safeguards and training are implemented.

6.4.3 *Practical Implications for SME Owners*

- Consider open-source and cloud-based cybersecurity tools for affordability.
- Build relationships with MSSPs to outsource critical security tasks.
- Conduct cybersecurity training for all staff, even basic awareness sessions.
- Engage in industry-specific forums to stay abreast of sector-relevant threats.

6.4.4 *Simplify Regulatory Requirements for SMEs*

- While compliance with data protection laws is crucial, policymakers should consider simplifying regulatory requirements for smaller enterprises without compromising data security standards. Simplified compliance requirements can reduce the operational burden on SMEs, particularly those without dedicated cybersecurity teams, and allow them to focus more on improving technical defences. Below are some of the examples of the initiatives that can be done.
    - Releasing compliance checklists, templates, and self-assessment tools tailored for SMEs to help them understand and meet regulatory requirements without needing extensive legal support.

    - Providing automated compliance reporting tools to streamline regulatory submissions and reduce administrative burdens.
    - Developing sector-specific cybersecurity toolkits that offer practical guidance on meeting compliance standards while addressing industry-specific risks.
    - Hosting workshops or webinars in collaboration with industry experts to educate SMEs on regulatory changes and best practices for compliance.

- Implementing zero-trust principles also supports regulatory compliance, as seen in frameworks like POPIA and FSCA standards. These regulations demand stringent access controls and data protection measures, which zero trust inherently provides. By adopting phishing-resistant MFA and micro-segmentation, SMEs can strengthen their compliance posture and reduce risks associated with non-compliance penalties.

6.5 Limitations of the Study

- The study had a sample size of thirteen, which may not represent the broader diversity of SMEs across all regions in South Africa. This limitation could affect the generalisability of the findings.
- The focus on specific sectors such as financial services, retail, manufacturing, and mining may limit the applicability of the findings to other industries, which might face unique cybersecurity challenges.
- The study primarily explored technical measures, and did not delve deeply into organisational policies or the human factors that impact cybersecurity readiness, which may also play a significant role.

- The methodological limitations included sample size, possible participant bias, and limited sectoral representation. Additionally, the study did not focus on governance structures or broader compliance frameworks. Future research can expand on these areas using mixed methods or cross-national comparisons.

6.6 Amended Framework

The amended conceptual framework reflects the findings of the study, validating some theoretical expectations while introducing new insights into SME cybersecurity practices. Regulatory pressures emerged as a critical driver for adopting cybersecurity measures, particularly in the financial services sector, where compliance with laws like POPIA and FSCA standards is mandatory. Technical expertise was confirmed to be a key enabler, with SMEs increasingly reliant on external service providers to bridge internal capability gaps. However, the findings also revealed new dimensions: financial constraints not only hinder adoption but also lead SMEs to depend on basic tools, leaving their cybersecurity defences inadequate. Moreover, psychological barriers, such as decision paralysis caused by the complexity of cybersecurity options, underscore the importance of incorporating behavioural perspectives into future frameworks. These insights refine the initial conceptual model by emphasising external support and behavioural factors as integral components of SME cybersecurity strategies. Below is the refined diagram of Figure 3-1 (in chapter 3).

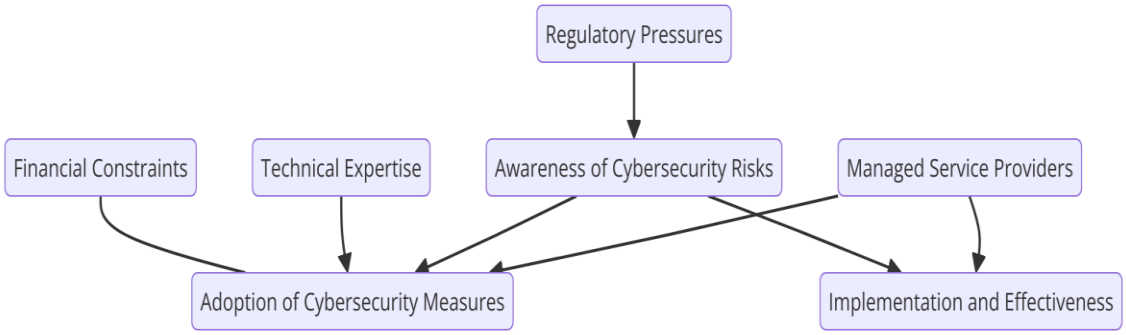


Figure 6-2: Amended Conceptual Model.

6.7 Suggestions for Future Research

AI and SME Cybersecurity Strategies

Future studies could explore the impact of emerging technologies like artificial intelligence and zero trust on SME cybersecurity strategies. Examining the effectiveness of AI in automating network monitoring, detecting intrusions, and mitigating threats could provide valuable insights for SMEs looking to enhance their cybersecurity posture.

SMEs should adopt a phased zero-trust implementation to enhance cybersecurity without overwhelming resources. Starting with cost-effective measures like leveraging built-in zero-trust tools in cloud services and deploying phishing-resistant MFA can offer immediate benefits. As the article highlights, “Zero trust minimises the potential damage that an insider can cause both intentionally and unintentionally.” (Collard, 2025) SMEs must also prioritise employee training to align with the cultural shift required for zero-trust adoption. Participant twelve noted, "Our staff are unfamiliar with advanced security protocols," reinforcing the need for awareness and education programs.

Regional Comparative Studies

Comparative studies across different African countries could provide insights into regional variations in cybersecurity challenges and solutions. Such research would help understand the unique constraints and opportunities in various contexts and could inform targeted policy interventions.

Exploring Organisational and Human Factors

Future research could also investigate the impact of organisational culture and human factors on cybersecurity readiness in SMEs. Understanding the role of employee awareness, behaviour, and leadership support could help design more comprehensive cybersecurity strategies that go beyond technical solutions.

6.8 Conclusion

This research highlights the critical need for robust cybersecurity measures tailored to the unique challenges faced by SMEs in South Africa. The findings reveal that while some SMEs, particularly in financial services, have adopted more comprehensive measures, the majority rely on basic protections that fail to address the sophistication of modern cyber threats. Financial constraints, limited expertise, and regulatory compliance remain persistent barriers to effective cybersecurity implementation.

Notably, sectoral differences impact cybersecurity readiness. For instance, in the manufacturing sector, there is less regulatory pressure compared to the financial sector, which faces stringent compliance requirements such as POPIA and FSCA standards. As a result, manufacturing SMEs often do not prioritise cybersecurity due to a lack of external regulatory drivers, while financial services SMEs are compelled to meet strict security standards to maintain regulatory compliance. This disparity underscores the importance of sector-specific approaches to cybersecurity solutions.

The analysis underscores the importance of integrating AI-driven solutions for continuous threat monitoring and rapid response, particularly for SMEs with limited in-house expertise. Partnerships with managed service providers and leveraging open-source cybersecurity tools offer viable pathways to bridge these gaps. Furthermore, aligning cybersecurity initiatives with industry regulations such as POPIA can foster better compliance and resilience. However, it is crucial to recognise that these solutions will differ or have variations for each sector of SMEs, reflecting their unique operational needs, regulatory pressures, and resource capacities.

The findings call for a multifaceted approach to SME cybersecurity enhancement, including targeted training programs, subsidies for advanced cybersecurity tools, and sector-specific best practices

Policymakers and industry stakeholders must work collaboratively to reduce barriers to cybersecurity adoption and create an enabling environment for SMEs to thrive in an increasingly digital economy. This collaboration should involve concrete actions such as private sector investment in cybersecurity capacity-building programs, funding subsidised training initiatives, and providing discounted access to security tools and services through public-private partnerships. Additionally, industry leaders can support sector-specific pilot programs to evaluate and refine cybersecurity solutions tailored for SMEs while policymakers facilitate regulatory sandboxes to ease compliance. Together, these targeted actions will address financial, technical, and regulatory barriers, fostering a more secure and resilient digital economy for SMEs.

Beyond this current research, the future studies can look at exploring emerging technologies, such as AI-powered threat detection and cloud-based security platforms, as well as analysing best practices for implementing these tools within resource-constrained SME environments. Comparative studies between various geographical areas can also look into how diverse industry support initiatives, regulatory frameworks, and public-private partnerships affect the uptake and efficacy of cybersecurity. Focusing on technical innovation and strategic

implementation will provide comprehensive insights to support SMEs in enhancing their cybersecurity resilience. Such efforts will provide a broader understanding of SME specific challenges and opportunities in safeguarding digital assets against evolving cyber threats.

REFERENCES

Ahmed, N. N., & Nanath, K. (2021). Exploring Cybersecurity Ecosystem in the Middle East: Towards an SME Recommender System. *Journal of Cyber Security and Mobility*, *10_3*, 511-536. https://doi.org/ 10.13052/jcsm2245-1439.1032

Akhtar, S., Sheorey, P. A., & Bhattacharya, S. (2021). Cyber Security Solutions for Businesses in Financial Services:Challenges, Opportunities, and the Way Forward. *International Journal of Business Intelligence Research*, *12*(1). https://orcid.org/0000-0003-3069-1976

Alahmari, A., & Duncan, B. (2020). *Cybersecurity Risk Management in Small and Medium-Sized Enterprises: A Systematic Review of Recent Evidence* Conference: 2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA),

Alahmari, A. A., & Duncan, R. A. (2021). *Investigating Potential Barriers to Cybersecurity Risk Management Investment in SMEs* 13th International Conference on Electronics, Computers and Artificial Intelligence (ECAI) | 978-1-6654-2534-6/21/,

Alexander, R. (2021). *Key Opportunities and Challenges for 4IR in South Africa. SARChI Industrial Development Working Paper Series WP 2021-8d*. University of Johannesburg.

Alharbi, F., Alsulami, M., AL-Solami, A., Al-Otaibi, Y., Al-Osimi, M., Al-Qanor, F., & Al-Otaibi, K. (2021). The Impact of Cybersecurity Practices on Cyberattack Damage:The Perspective of Small Enterprises in Saudi Arabia. *Sensors*.

Aliyu, A. A., Singhry, I. M., Adamu, H., & Abubakar, M. a. M. (2015). *ONTOLOGY, EPISTEMOLOGY AND AXIOLOGY IN QUANTITATIVE AND QUALITATIVE RESEARCH: ELUCIDATION OF THE RESEARCH PHILOPHICAL MISCONCEPTION*

Amrin, N. (2014). *The Impact of Cyber Security on SMEs* University of Twente].

Armenia, S. (2021). A dynamic simulation approach to support the evaluation of cyber risks and security investments in SMEs *Decision Support Systems*. https://doi.org/ https://doi.org/10.1016/j.dss.2021.113580

Ashfaq, S., Chandre, P., Pathan, S., Mande, U., Nimbalkar, M., & Mahalle, P. (2024). *Defending Against Vishing Attacks: A Comprehensive Review for Prevention and Mitigation Techniques*

Aygun, A., Sevinc, Q., Sadat, F., Efsane, H., & Mecid, Q. (2022). EFFECTS OF CYBER ATTACKS ON SMALL AND MEDIUM ENTERPRISES (SMEs). *The Baltic Scientific Journal*, *59*(1).

Bhattacharya, D. (2015). *Evolution of Cybersecurity Issues In Small Businesses* the 4th Annual ACM Conference,

Botha, J. G., Eloff, M. M., & Swart, I. (2015). The Effects of the PoPI Act on Small and Medium Enterprises in South Africa https://researchspace.csir.co.za/items/3650b3f2-485d-4c3b-aee2-e17beaaad180

Chingoriwo, T. (2022). Cybersecurity Challenges and Needs in The Context of Digital

Development in Zimbabwe. *British Journal of Multidisciplinary and Advanced Studies: Engineering and Technology*, *3(2)*, 77-104. https://doi.org/ https://doi.org/10.37745/bjmas.2022.0046

Clarke, V., & Braun, V. (2017). Thematic analysis. *The Journal of Positive Psychology*, *12*(3).

Cobos, E. V. (2024). *CYBERSECURITY ECONOMICS FOR EMERGING MARKETS*. https://documents1.worldbank.org/curated/en/099091624175097991/pdf/P17876915bd69a0671b2f2166697a1c7793.pdf

Collard, A. (2025). *Why is Zero-Trust Approach Critical for SMEs?* Retrieved January 7 from https://www.itnewsafrica.com/2025/01/why-is-zero-trust-approach-critical-for-smes

Cook, K. D. (2017). *Effective Cyber Security Strategies for Small Businesses* Walden University].

Costa, W. J. D. (2024). *CIPC cyber attack leaves millions of entities vulnerable across South Africa*. Cape Chamber of Commerce and Industry. Retrieved July from https://capechamber.co.za/latest-news/cipc-cyber-attack-leaves-millions-entities-vulnerable-across-south-africa

Cruz, E. D. L., Hyatt, J. C., Nadella, G. S., Gonaygunta, H., Meduri, S. S., & Cruz, A. M. D. L. (2024). *Government Cybersecurity Data Analytics System Success: An Exploratory Study of Technology and Organization* International Symposium on Networks, Computers and Communications (ISNCC), Washington DC, DC, USA.

Department for Science, I. T. (2024). *Official Statistics Cyber security breaches survey 2024*. UK GOVERMENT. Retrieved July from https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024/cyber-security-breaches-survey-2024

Erdogan, G., Halvorsrud, R., Boletsis, C., Tverdal, S., & Pickering, J. B. (2023). *Cybersecurity Awareness and Capacities of SMEs* In Proceedings of the 9th International Conference on Information Systems Security and Privacy

Eybers, S., & Mvundla, Z. (2021). Investigating Cyber Security Awareness (CSA) amongst Managers in Small and Medium Enterprises (SMEs). In: University of Pretoria, Private Bag X20, Hatfield, Pretoria, South Africa.

Fallatah, W., Kävrestad, J., & Furnell, S. (2024). Establishing a Model for the User Acceptance of Cybersecurity Training. *Future Internet*, 294. https://doi.org/ https://doi.org/10.3390/fi16080294

Fortinet. (2024). *Notice of Recent Security Incident*. Retrieved 25 January from https://www.fortinet.com/blog/business-and-technology/notice-of-recent-security-incident

Forum, W. E. (2024). *Navigating Cyber Resilience in the Age of Emerging Technologies: Collaborative Solutions for Complex Challenges*. https://www.weforum.org/publications/navigating-cyber-resilience-in-the-age-of-emerging-technologies-collaborative-solutions-for-complex-challenges/

Good, N. (2019). Using behavioural economic theory in modelling of demand response. *Applied Energy*, *239*, 107-116. https://doi.org/https://doi.org/10.1016/j.apenergy.2019.01.158

ITWEB. (2024). *Financial sector faces pressure to meet FSCA Cyber Resilience Standards*. Retrieved 23 January from https://www.itweb.co.za/article/financial-sector-faces-pressure-to-meet-fsca-cyber-resilience-standards/lwrKxv3YgAyMmg1o

Kabanda, S., Tanner, M., & Kent, C. (2018). Exploring SME cybersecurity practices in developing countries. *Journal of Organizational Computing and Electronic Commerce,*.

Kansal, A., & Saha, S. (2023). The intention of Fintech adoption in TAM perspective: A SEM approach. *Journal of Statistics and Management Systems*, *26*(3), 505-514. https://doi.org/https://doi.org/10.47974/JSMS-1043

Kariuki, P., Ofusori, L. O., & Subramaniam, P. R. (2023). Cybersecurity threats and vulnerabilities experienced by small-scale African migrant traders in Southern Africa. *Security Journal*. https://doi.org/https://doi.org/10.1057/s41284-023-00378-1

Kaur, R., Gabrijelˇciˇc, D. s., & Klobuˇcar, T. z. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. *Elsevier Information Fusion 97*. https://doi.org/10.1016/j.inffus.2023.101804

Korstjens, I., & Moser, A. (2017). Series: Practical guidance to qualitative research. *European Journal of General Practice*. https://doi.org/ DOI: 10.1080/13814788.2017.1375092

Lindemulder, G., & Kosinski, M. (2024). Retrieved 05 January from https://www.ibm.com/think/topics/cybersecurity?utm_source=chatgpt.com

Lloyd, G. (2020). The business benefits of cyber security for SMEs In: Computer Fraud & Security.

Malinga, S. (2025). *Cell C accuses 'unauthorised party' of data breach*. Retrieved 15 January from https://www.itweb.co.za/article/cell-c-accuses-unauthorised-party-of-data-breach/5yONP7ErQneMXWrb

Manzoor, J., Waleed, A., Jamali, A. F., & Masood, A. (2024). Cybersecurity on a budget: Evaluating security and performance of open-source SIEM solutions for SMEs. *PLOS ONE*, *19(3)*(e0301183). https://doi.org/.

https://doi.org/10.1371/journal.pone.0301183

Mbatha, B. (2024). Digital divide: a phenomenon of unequal adoption of technology by SMMEs in the agribusiness sector in South Africa. *Sabinet African Journals*, *43*(2). https://journals.co.za/doi/full/10.36615/vdjgg265?utm_source=chatgpt.com

Moyo, A. (2024a). *Capitec restores services after Crowdstrike outage*. Retrieved 21 January from https://www.itweb.co.za/article/capitec-restores-services-after-crowdstrike-outage/WnpNgM21pl17VrGd

Moyo, A. (2024b). *Justice department suffers another cyber attack*. Retrieved July from https://www.itweb.co.za/article/justice-department-suffers-another-cyber-attack/rW1xLv5nJkx7Rk6m

Münter, M. T. (2024). Resource Based View. *ScienceDirect*. https://doi.org/https://doi.org/10.1016/B978-0-443-13701-3.00203-6

Naude, M., Martins, I., & Singh, U. G. (2023). *GLOBAL TRENDS IN MANAGEMENT,IT AND GOVERNANCE IN AN e-WORLD* eMIG 2023, Hybrid and in person Mauritius.

Ncubukezi, T. (2023). *DESIGN DEVELOPMENT AND EVALUATION OF THE CYBERSECURITY RISK TOOL: A CASE OF SMALL AND MEDIUM-SIZED ENTERPRISES IN SOUTH AFRICA* Cape Peninsula University of Technology]. Bellville.

O'Niell, C., Troha, C., Lyon, V., Holstege, B., Asen, A., Geoffrey Cheung, Y. S., & Mitchell, S. (2024). *What Cybersecurity Leaders Get Right*. https://www.bcg.com/publications/2024/what-cybersecurity-leaders-get-right

Puchert, D. (2024). South African R49 million cybersecurity pain. Retrieved 22 October 2024, from https://mybroadband.co.za/news/security/564705-south-africa-r49-million-cybersecurity-pain.html

PWC. (2021). *Threat digest: Emerging cyber threats in the manufacturing and mining sectors*.

PWC. (2024). *South Africa and Africa Report - Global Digital Trust Insights Survey 2025*. https://www.pwc.co.za/en/publications/digital-trust-insights.html

Rawindaran, N., Jayal, A., & Prakash, E. (2021). Machine Learning Cybersecurity Adoption in Small and Medium Enterprises in Developed Countries. *Computers*, *10*. https://doi.org/10.3390/computers10110150

Rawindaran, N., Jayal, A., Prakash, E., & Hewage, C. (2023). Perspective of small and medium enterprise (SME's) and their relationship with government in overcoming cybersecurity challenges and barriers in Wales. *International Journal of Information Management Data Insights*, *100191*. https://doi.org/https://doi.org/10.1016/j.jjimei.2023.100191

Renaud, K., & Ophoff, J. (2021). A cyber situational awareness model to predict the implementation of cyber security controls and precautions by SMEs. *Emerald*, *1*(1), 24-26. https://doi.org/10.1108/OCJ-03-2021-0004

Sang, K. (2023). *CYBERSECURITY ASSESSMENT MODEL FOR SMALL AND MEDIUM ENTERPRISES (SMEs) E-COMMERCE IN KENYA* KCA UNIVERSITY].

SEDA. (2023). *SMME Quarterly Update 3rd Quarter* https://www.ber.ac.za/BER%20Documents/Manufacturing-Survey/?doctypeid=1067

UJ-TRCTI. (2022). *Emerging Technologies in South Africa: A Landscape Analysis.* . University of Johannesburg.

Varachia, M. (2022). *Adoption of cybersecuroty practices for SMMES* University of Johannesburg].

Wolford, B. *What is GDPR, the EU's new data protection law?* GDPR.EU. Retrieved July from https://gdpr.eu/what-is-gdpr/

Wonglimpiyarat, J., & Yuberk, N. (2005). In support of innovation management and Roger's Innovation Diffusion theory. *ScienceDirect*, *22*(3), 411-422.

World Bank. (2019, 16 October 2019). *Small and Medium Enterprises (SMEs) Finance*. Retrieved 12 April from https://www.worldbank.org/en/topic/smefinance

World Economic Forum. (2024, 22 February). *3 trends set to drive cyberattacks and ransomware in 2024*. Retrieved 12 April from https://www.weforum.org/agenda/2024/02/3-trends-ransomware-2024/

World Economic Forum. (2025). *Global Cybersecurity Outlook 2025 – Navigating Through Rising Cyber Complexities*. Retrieved 22 January from

https://www.weforum.org/press/2025/01/global-cybersecurity-outlook-2025-navigating-through-rising-cyber-complexities/

Yudhiyati, R., & Putritama, A. (2021). What small businesses in developing country think of cybersecurity risks in the digital age:Indonesian case. *Journal of Information,Communication and Ethics in Society*, *19*(4), 446-462.

APPENDIX (A) Instrument

Interview guide

Section 1: Identifying Technical Cybersecurity Measures

1. Current Cybersecurity Measures

- Can you walk me through the technical cybersecurity measures your organisation currently has in place?
- How do you approach the configuration and management of firewalls in your organisation?
- Could you elaborate on your use of Intrusion Detection Systems (IDS), if any? How are these systems integrated into your overall security strategy?
- What encryption protocols do you use for securing data, both at rest and in transit?
- How do you ensure the security of individual devices within your organisation? What types of endpoint security software do you rely on?

2. Adoption of Cybersecurity Technologies

- What were the main factors that influenced your decision to implement these specific cybersecurity measures?
- How long has your organisation been utilising these cybersecurity measures, and what prompted their initial adoption?

Section 2: Evaluating the Effectiveness of Cybersecurity Measures

3. Effectiveness of Current Measures

- In your experience, how effective are your current cybersecurity measures in protecting against cyber threats?

- Can you share any specific incidents where these measures successfully prevented a cyber-attack?
- Have you encountered any breaches or incidents despite having these measures in place? If so, can you describe what occurred and how your organisation responded?

4. Monitoring and Updates

- How often do you review and update your cybersecurity measures to ensure they remain effective?
- What metrics or benchmarks do you use to assess the effectiveness of your cybersecurity measures?

Section 3: Challenges in Implementing Cybersecurity Measures

5. Implementation Challenges

- What challenges did you encounter during the implementation of your current cybersecurity measures?
- Were there any technical challenges that were particularly difficult to overcome? How did you address them?
- How did financial constraints influence your ability to implement comprehensive cybersecurity measures?

6. Maintenance and Management Challenges

- What ongoing challenges do you face in maintaining and managing your cybersecurity measures?
- Do you have dedicated IT staff or cybersecurity professionals to manage these measures? If not, how is this responsibility handled?

7. Training and Awareness

- How would you describe the level of cybersecurity awareness among your employees?
- Do you conduct regular cybersecurity training for your staff? If so, how do you evaluate the effectiveness of these training sessions?

Section 4: Strategies and Best Practices

8. Optimising Cybersecurity

- What strategies have you found most effective in optimising the deployment and utilisation of your cybersecurity measures?
- Have you adopted any cost-effective solutions that have enhanced your cybersecurity posture?
- How do you stay informed about the latest cybersecurity threats and best practices?

9. Recommendations

- Based on your experience, what best practices would you recommend to other SMEs looking to improve their cybersecurity measures?
- Are there any specific tools or technologies you believe are particularly beneficial for SMEs in the South African market?

10. Plans

- Do you have any plans to upgrade or enhance your current cybersecurity measures soon? If so, what are they?

APPENDIX (B) Consent Form

Title of project: Exploring Technical Implementation of Cybersecurity Measures within Small and Medium Enterprises (SMEs) in the South African Market

Name of researcher: Dineo Baloyi

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

I agree to the following:

(Please circle the relevant options below)

The research study was explained to me. I understand what this study is about.	YES	NO
I understand that I can volunteer to take part in the study	YES	NO
I agree that the interview may be audio recorded	YES	NO
I agree that direct quotations from my interview may be used by the researcher in their research report	YES	NO
I agree that my participation will remain anonymous (my name or other identifying data will not be used by the researcher in their research report	YES	NO

I agree that other researchers may use the information I provide in my interview (depending on their own ethics clearance being obtained) but my name and any personal information will not be used or passed on	YES	NO

…… (signature)

…… (name of participant)

…… (date)

APPENDIX (C) Participation Information Sheet

Dear Sir / Madam

My name is Dineo Monicca Baloyi. I am a Master of Management in Digital Business student at the University of the Witwatersrand, Johannesburg. My supervisor is Dr Zubeida Dawood. I am conducting a research study about Cybersecurity. The study title is ''Exploring Technical Implementation of Cybersecurity Measures within Small and Medium Enterprises (SMEs) in the South African Market''.

I am inviting you to take part in an interview. If you decide to take part, your participation in this research study will last about one hour. The interview will take place at a location of your choosing or online at the agreed.

With your permission, I would like to audio record the interview. This data will be stored in an encrypted/password protected folder on my laptop for duration of the research and/or deleted after the outcome of the degree. Only I will have access to the data.

The interview will be confidential and anonymous. When I share the results of the research study, I will not include your name or anything else that could identify you. With your permission, other researchers may use the data collected from this research study, but your name and any personal information will not be used or passed on.

If you decide to take part in the research study, it should be because you want to volunteer. You do not have to take part. You can stop being in the study at any time. You do not have to answer any questions if you do not want to. You will not get any direct benefits if you choose to join the research study. You will not lose any services, benefits or rights you would normally have if you decided not to join. Taking part in the research study will not cost you anything. You will not be paid for being in this research study.

The risks for this research study are no more than what happens in everyday life OR some of the questions asked may make you feel sad or upset. If this happens, I will stop the interview and continue another time. If you need some support or counselling services following the interview, I will reach out to a nearest community-based support nearest to you.

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)117171408, email hrecnon-medical@wits.ac.za.

Yours sincerely,

Dineo

Researcher:

Dineo Monicca Baloyi, 0714395m@students.wits.ac.za, 082 437 6985

Supervisor:

Dr Zubeida Dawood, zubeida.dawood@wits.ac.za

APPENDIX (D) Ethics Approval Letter

Graduate School of Business Administration
University of the Witwatersrand, Johannesburg

Wits Business School

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

Ethics Clearance Certificate

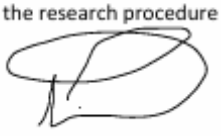
Ethics protocol number: WBS/DB0714395M/996
This certificate is only valid with a legitimate ethics protocol number and signed by the Researcher (below).

Project title	Exploring Technical implementation of cybersecurity measures within small and medium enterprises (SMEs) in the South African market
Investigator / Researcher	Mrs Dineo Baloyi
Nature of Project	MM (Digital Business)
Decision of the Committee	Approved, provided stakeholders and participants are guaranteed confidentialty.
Issue Date of Certificate	02/09/2024
Expiry date	Date of submission of the project / research report
Chairperson	Dr Ayanda Magida ☎ +27 11 717 3953 ✉ ayanda.magida@wits.ac.za

Declaration by Researcher

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

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



Signature

03/09/2024

Date: