

https://dspace.org/

An investigation of cybersecurity implementation challenges among South African SMEs

Fakir, Jeeten

2024
University of the Witwatersrand, Johannesburg
https://hdl.handle.net/10539/44227
Fakir, Jeeten. (2024). An investigation of cybersecurity implementation challenges among South African SMEs [Master's dissertation, University of the Witwatersrand, Johannesburg]. WireDSpace.https://hdl.handle.net/10539/44227

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

An investigation of cybersecurity implementation challenges among South African SMEs

Jeeten Fakir

2594644

2594644@students.wits.ac.za / 0832121381

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

In today's technologically driven world, cybersecurity implementation among Small and Medium Enterprises (SMEs) is of paramount importance, particularly in developing nations like South Africa, where cybercrime is prevalent. Due to inadequate cybersecurity practices, weak policy execution, and low public awareness, cybercriminals are targeting South Africa. Furthermore, local SMEs have limited budget, skills and resources dedicated to cybersecurity, which enhances the problem in the current South African context. Drawing upon a literature review encompassing global perspectives on cybersecurity and SMEs, this study focuses on the South African context to provide insights tailored to the local SME landscape.

This research investigates the cybersecurity implementation challenges faced by SMEs, by exploring the influence that subjective norms, attitude, perceived behavioural control, perceived ease of use, and perceived usefulness has on the intention to implement cybersecurity among South African SMEs. This quantitative study employed a survey which was distributed on social media to SMEs across the country to answer the research objectives. Key findings highlight the significant gaps in cybersecurity awareness and resources among South African SMEs, underscoring the urgent need for enhanced cybersecurity education and support. The investigation indicates that subjective norms, attitude, perceived behavioural control, perceived ease of use, and perceived usefulness contribute significantly to influencing cybersecurity implementation among South African SMEs. The identified factors provide a foundation for addressing the research objectives by emphasising the importance of subjective norms, attitudes, control perceptions, ease of use, and usefulness perceptions in the context of cybersecurity implementation. Ultimately, this research underscores the imperative for collaborative efforts between government, academia, and industry to address cybersecurity challenges faced by South African SMEs and foster a more resilient digital ecosystem.

KEYWORDS

cybersecurity, cyber threats, cyberattacks, South Africa, small and medium enterprises (SMEs), cybersecurity frameworks

DECLARATION

I, Jeeten Fakir, 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: Jeeten Fakir Signature:

Signed at ……Brackenhurst, Johannesburg……

On the ……28…….. day of …February…… 2024…..

DEDICATION

This research report is dedicated to my late mother, Manjular Fakir, and my father, Chandoolal Fakir, for their constant support and prayers.

ACKNOWLEDGEMENTS

First and foremost, I thank the Almighty God for blessing me with the opportunity to partake in this master's programme, and for giving me the strength, discipline, and courage to see it through.

I thank my wife, Alicia Fakir, for her unwavering support, love, and encouragement. Without her support, this journey would not have been possible. I also thank my children, Hrihaan and Taheer, for their understanding when I could not be present at home, or at school and family occasions.

My sincere gratitude goes to my supervisor, Dr Eleanor Meda Chipeta, for her wisdom, guidance, and insightful advice. Her supervision, timeous feedback, and suggestions were invaluable in ensuring this research report is a success.

I thank all the SME Owners who took the time out of their busy schedules to complete my survey, with the acknowledgement that this study would not have been possible without their valuable input.

TABLE OF CONTENTS

LIST OF TABLES x

LIST OF FIGURES xii

LIST OF ACRONYMS xiii

CHAPTER 1. INTRODUCTION 1

1.1 STATEMENT OF PURPOSE 1
1.2 BACKGROUND TO THE STUDY 1
1.3 CONTEXT OF STUDY 3
1.4 PROBLEM STATEMENT 9
1.5 RESEARCH OBJECTIVE 10
1.6 THEORETICAL FRAMEWORK 10
1.7 RATIONALE 11
1.8 DELIMITATIONS OF THE STUDY 12
1.9 DEFINITION OF TERMS 13
1.10 ASSUMPTIONS 13
1.11 CHAPTER OUTLINE 14

CHAPTER 2. LITERATURE REVIEW AND THEORETICAL FRAMEWORK 15

2.1 INTRODUCTION 15
2.2 TREND IN CYBERSECURITY RESEARCH 15
2.3 UNDERSTANDING CYBERCRIME AND CYBERSPACE 24
2.3.1 CYBERCRIME 24
2.3.2 CYBERSPACE 26
2.4 CYBERSECURITY 28
2.5 IMPACT OF CYBER THREATS ON SMES 30
2.5.1 TYPES OF CYBER THREATS 31
2.6 CYBERSECURITY FRAMEWORKS 35
2.6.1 NIST CSF FRAMEWORK 36
2.6.2 KING IV REPORT 39
2.7 THEORETICAL FRAMEWORK 40
2.7.1 THEORY OF PLANNED BEHAVIOUR (TPB) 41
2.7.2 TECHNOLOGY ACCEPTANCE MODEL (TAM) 44
2.8 CONCEPTUAL FRAMEWORK 46

2.9 Conclusion of Literature Review 47

CHAPTER 3. RESEARCH METHODOLOGY 48

3.1 Research approach 48
3.2 Research design 49
3.3 Data collection methods 49
3.4 Population and sample 50
3.4.1 Target population 50
3.4.2 Sample and sampling method 50
3.5 The measuring instrument 52
3.6 Procedure for data collection 53
3.7 Data analysis strategies and interpretation 54
3.8 Possible limitations and challenges of the study 56
3.9 Quality Assurance 56
3.9.1 External validity OR transferability 56
3.9.2 Internal validity OR credibility 56
3.9.3 Reliability OR dependability 57
3.10 Ethical considerations 57
3.11 Proposed schedule and timelines 57

CHAPTER 4. PRESENTATION AND INTERPRETATION OF RESULTS 59

4.1 Introduction 59
4.2 Results pertaining to Research Objective 59
4.2.1 Reliability Analysis 59
4.2.2 Descriptive Analysis 62
4.2.3 Correlation Analysis 71
4.2.4 Factor Analysis 73
4.2.5 ANOVA Test 83
4.3 Discussion of results 85

CHAPTER 5. CONCLUSIONS & RECOMMENDATIONS 89

5.1 Introduction 89
5.2 Conclusions regarding the research objectives 90
5.2.1 Implications considering the technological, economic and social issues 92
5.3 Recommendations 93
5.3.1 Enhance perceived ease of use through training and user-friendly tools 93
5.3.2 Emphasize perceived usefulness through awareness and with demonstrated benefits 95

5.3.3 FOSTER POSITIVE ATTITUDES TOWARDS CYBERSECURITY THROUGH LEADERSHIP, CLEAR COMMUNICATION, AND CULTURE 96
5.3.4 FACILITATE PERCEIVED BEHAVIOURAL CONTROL WITH RESOURCES AND SUPPORT 96
5.3.5 LEVERAGE SUBJECTIVE NORMS THROUGH PEER INFLUENCE AND INDUSTRY STANDARDS 97
5.3.6 ENCOURAGE CYBERSECURITY PARTNERSHIPS ACROSS ALL STAKEHOLDERS 97
5.4 LIMITATIONS 98
5.5 SUGGESTIONS FOR FURTHER RESEARCH 99

REFERENCES 101

APPENDIX A: PARTICIPATION INFORMATION SHEET 116

APPENDIX B: CONSENT FORM 117

APPENDIX C: QUESTIONNAIRE 118

APPENDIX D: ETHICS CLEARANCE CERTIFICATE 140

LIST OF TABLES

Table 1 – NIST functions and categories

Table 4.1 – Subjective norms reliability analysis

Table 4.2 – Attitude reliability analysis

Table 4.3 – Perceived behavioural control reliability analysis

Table 4.4 – Perceived ease of use reliability analysis

Table 4.5 – Perceived usefulness reliability analysis

Table 4.6 – Correlation analysis

Table 4.7 – Subjective norms total variance

Table 4.8 – Subjective norms communalities

Table 4.9 – Attitude total variance

Table 4.10 – Attitude communalities

Table 4.11 – Perceived behavioural control total variance

Table 4.12 – Perceived behavioural control communalities

Table 4.13 – Perceived ease of use total variance

Table 4.14 – Perceived ease of use communalities

Table 4.15 – Perceived usefulness total variance

Table 4.16 – Perceived usefulness communalities

LIST OF FIGURES

Figure 1 – The cyberattack taxonomy

Figure 2 – The Theory of Planned Behaviour

Figure 3 – The Technology Acceptance Model

Figure 4 – Conceptual framework

Figure 5 – Research report project plan

Figure 6 – Age descriptive analysis

Figure 7 – Gender descriptive analysis

Figure 8 – Nationality descriptive analysis

Figure 9 – Race descriptive analysis

Figure 10 – Education descriptive analysis

Figure 11 – Field of study descriptive analysis

Figure 12 – Number of employees descriptive analysis

Figure 13 – Industry descriptive analysis

LIST OF ACRONYMS

COBIT – Control Objectives for Information Technologies

ISO – International Organisation for Standards

ITIL – Information Technology Infrastructure Library

NIST CSF – National Institute of Standards and Technology Cybersecurity Framework

SME – Small and Medium Enterprise

TAM – Technology Acceptance Model

TPB – Theory of Planned Behaviour

CHAPTER 1. INTRODUCTION

1.1 Statement of purpose

The purpose of this research is to investigate cybersecurity implementation challenges among South African SMEs. This study intends to investigate the influence that perceived ease of use, perceived usefulness, attitude, perceived behavioural control, and subjective norms has on the implementation of cybersecurity among SMEs in South Africa.

1.2 Background to the study

The current technological landscape is experiencing a significant surge, with the Fourth Industrial Revolution leading the way towards seamless digital interactions that transcend geographical borders (Ng & Ghobakhloo, 2020). Society and enterprises are increasingly influenced by technological progressions, leading to a range of advantages for organisations, including novel business models, expansion into global target markets, cost efficiencies, and enhanced customer experiences (Rawindaran et al., 2022). Nonetheless, the digital era has presented certain challenges, a major one being the issue of increased cybercrime globally (Bada & Nurse, 2019). Accordingly, information security and cybersecurity, and the management thereof, are crucial considerations within organisations of today (Antunes et al., 2022).

During the World Economic Forum's annual meeting on cybersecurity in November 2022, cybersecurity experts expressed apprehensions regarding the existing disparity in cybersecurity capabilities between SMEs and larger organisations. The experts noted that SMEs are at a greater risk of falling victim to cyberattacks due to a lack of adequate cybersecurity skills, potentially resulting in significant financial repercussions for these entities (World Economic Forum, 2023). The deliberations centred on the notion that SMEs may lack the necessary

capacity to respond effectively to such cyber threats. Similar sentiments are shared by various researchers. For example, Hoong and Rezania (2024) highlight five significant disputes affecting the discussions on cybersecurity in SMEs. These disputes include differing views on cybersecurity and privacy, disparities in education levels, financial limitations, conflicting responsibilities with third-party providers, and inadequate government communication (Hoong & Rezania, 2024). Similarly, Baba and Nurse (2019) highlight that SME owners' immersion in daily business operations could also contribute to cybersecurity struggles. Furthermore, in an exploratory study conducted on the effect of cybersecurity awareness within SMEs in Wales, Rawindaran et al. (2022) indicate that only 30% of the 122 SME respondents sampled understood cybersecurity terminology, highlighting the low level of cybersecurity knowledge among SMEs. Consequently, there is a need for SMEs to understand concepts such as cyberspace, cybersecurity, cyber threats, and cybersecurity frameworks, which include risk mitigation strategies.

Cyber-attacks are on the rise in South Africa, and according to reports, South Africa is frequently listed in the top five countries for the most cyber-attacks (Kondlo et al., 2022). According to the Council for Scientific and Industrial Research (CSIR), cybercrime costs South Africa an estimated R2.2 billion annually and has a substantial detrimental effect on the economy (Mzekandaba, 2024). Like many economies worldwide, SMEs are a vital contributor to the South African economy (Kalidas et al., 2020). They contribute 39% to the country’s gross domestic product, represent 98% of the business workforce, contribute between 50-60% towards employment across industries, and are responsible for 25% of the job growth in the private sector (Kalidas et al., 2020). SMEs are increasingly utilising digital engagement platforms to engage in the global market and improve efficiency in their offerings (Hasanah et al., 2022). This does however increase their risk, the main issue being IT systems related, particularly cybersecurity concerns (Gunduz & Das, 2020). Globally, there is a theme that indicates that SMEs do not take cybersecurity seriously (Wilson et al., 2023). Developing countries face a greater risk of cyber-attacks, especially SMEs that

have limited resources to invest in cybersecurity measures, and those who lack the relevant IT capacity and capabilities (Tetteh & Otioma, 2024).

A study by Rawindaran et al. (2023), focused on SME cybersecurity strategies and the obstacles that they encounter, indicates that the perception of cybersecurity is constrained by internal factors such as management support, attitudes, and budget, as well as institutional pressures, and the cybersecurity environment (Rawindaran et al., 2023). In another study by Eybers et al. (2022), which investigated cybersecurity awareness within the management layer in South African SMEs, it was noted that lack of expertise and funding are a major hindrance for cybersecurity practises within SMEs (Eybers & Mvundla, 2022).. A study by Murphy et al. (2022), which looked at the factors that impede compliance with national cybersecurity policies within the SME space in South Africa, indicates that a lack of awareness and understanding of the policy, resource constraints and a lack of the perceived benefits of the relevant policies are the main factors (Murphy et al., 2022).

Even though the segment is of grave importance to the South African economy, there seems to be a gap in the academic sphere with regards to the factors which influence the behaviour to implement cybersecurity within SMEs in South Africa. There are practical views from management consulting firms, however there is limited academic literature on this topic. To highlight the issue – a search on Sabinet Online, a database of South African journals, for the keywords “cybersecurity” and “SME”, returns 11 journal articles. Therefore, this study seeks to investigate the factors that influence cybersecurity implementation, and to create cybersecurity awareness among SMEs in South Africa.

1.3 Context of study

In a technology-driven world, characterised by rapid evolution, encompassing social media, online transactions, cloud computing, and automated processes, businesses across industries face persistent risks with the continual rise in

cybercrime instances. Although the new digital era has led to new opportunities for businesses to reach wider audiences, improve operational efficiencies, and create new revenue streams, it also poses significant challenges for businesses, with cybercrime being at the top of the list (Mphatheni & Maluleke, 2022). Considering the escalating prevalence of cybercrime, businesses of all sizes are at risk of cyberattacks. While large enterprises have more resources to invest in cybersecurity, smaller businesses often encounter resource constraints due to the absence of an earmarked cybersecurity budget and requisite expertise, thereby impeding their ability to keep up the pace with evolving technologies and security threats. Consequently, they are frequently perceived as more vulnerable targets by cybercriminals (Gafni & Pavel, 2019).

A study by Mallick et al. (2024) highlights the fact that cyber criminals possess above-average knowledge of programming, operating systems, and system vulnerabilities, hence their ability to obtain unauthorised access to computer systems, networks, and data, to compromise the confidentiality, availability, and integrity of the information (Mallick & Nath, 2024). The ongoing development of new attack tools and methods, further provides cyber criminals with the advantage and makes it easier for them to plan attacks. Cybercrime also generates significant financial gains, which further motivates cyber criminals. Recent studies emphasize the immense economic consequences of cyber-attacks, quantified in trillions of dollars, and the trend continues to increase. These variables collectively contribute to the increasing frequency and complexity of cyber-attacks (Mallick & Nath, 2024).

Cyberattacks are becoming more severe and occur frequently on a global, national, and local level, as well as inside the South African public sector (Ngoma et al., 2021). Cybercriminals appear to believe that industries and businesses in South Africa are inadequately protected compared to first world countries, and they therefore take every opportunity to commit cybercrimes here. Cybercriminals compute the likelihood of being apprehended or receiving a light sentence if apprehended, and thus target South Africa due to its notoriety for its lax

cybercrime policy (Koigi, 2020; Mcanyana et al., 2020). Due to insufficient efforts to provide cybersecurity, the ineffective implementation of a policy framework, and a lack of public awareness on the cyberspace menace, cybercriminals have begun targeting South Africa (Mcanyana et al., 2020).

According to cybersecurity experts, Surfshark, South Africa is ranked 6th in the world in terms of cyber victims per one million internet users, and this costs the country R2.2 billion annually. In the same article, the Director of Cybersecurity at the University of Johannesburg, Basie von Solms, stated that cybercrime has now surpassed drug trafficking and arms dealing as the number one crime in the world (BusinessTech, 2022). Recent research by Accenture indicates that, out of the overall cyberattacks in South Africa, 43% are targeted at SMEs (Business Partners Limited, 2022).

A developing country such as South Africa, consistently encounters overwhelming obstacles. South Africa's cybersecurity defence is hindered by the inability to invest in cybersecurity practitioners, slow development of the relevant policies and legislation, lack of cybersecurity awareness, inexperience, and limited technical ability (Pieterse, 2021). Insufficient collaboration between the public and private sectors, and inadequacy of our law enforcement institutions in detecting and combating cybercrime, makes South Africa a prime target for cyber criminals (Shingange, 2022).

The South African government encounters significant difficulties in effectively regulating cybersecurity, particularly in terms of coordinating cybersecurity initiatives and safeguarding data across all levels of government, as well as regulators, businesses, and civil society. South Africa is renowned for its commendable legislation and policies on various matters, including the Cybercrimes Bill and POPI. Nevertheless, the country consistently faces its most significant obstacle in effectively executing these measures. The task of establishing a constructive cybersecurity culture lies with both the public and private sectors, who must collaborate and share collective accountability (Mabunda, 2021).

With regards to cybersecurity policy, the Ministry of State Security oversaw the implementation of the National Cybersecurity Policy Framework (NCPF), which was the government's response in 2015 (Mcanyana et al., 2020). In 2017, the National Assembly passed the Cybercrimes and Cybersecurity Bill, which was delayed due to the public's intense scrutiny of its impact on privacy and freedom of expression. In terms of cybersecurity legislation, government coordination, industry and citizen engagement, and the availability of trained labour, South Africa falls behind industrialised economies (Olaitan et al., 2021).

In addition, while the SAPS is now authorized to prosecute cybercrime offenses, a lack of cybercrime training poses challenges in the short term. The Protection of Personal Information (POPI) Act, which was instituted in 2013 to protect data privacy, is being implemented gradually, which further hinders the progress of the cybersecurity function in South Africa (Olaitan et al., 2021).

The current SME cohort in South Africa, who have constrained resources and limited capacity to develop ICT skills, and consequently require support from the government, poses a concern due to the government’s slow response to cybersecurity. Many schools lack the resources and teachers with the necessary ICT training, which is made worse by the fact that students don't have access to computers and the internet at home. Despite an increase in university graduations in computer science, this growth has been more slower than in other fields, in part due to ICT students' high dropout rates (Kirlidog et al., 2018).

Another issue is the adoption of appropriate cybersecurity practices by individuals, that requires a combination of education and awareness. Despite increasing internet usage and widespread worries about cybersecurity governance, there hasn't been anything done or thought to have been planned by government or business to date. Convincing businesses to take the necessary precautions to protect their assets, including the information they hold about their clients, from attacks and to notify any successful attacks presents a similar difficulty (Olaitan et al., 2021).

In summary, South Africa lags in implementing cybersecurity in relation to advanced economies. These delays have resulted in the lack of the necessary experience and the supply of skilled labour to the business world (Olaitan et al., 2021). This problem is further exacerbated by the large number of SMEs lack the budget or skills required to secure their businesses, while relying on already constrained government support (Kirlidog et al., 2018). SMEs are a crucial part of the South African economy, therefore ensuring their sustainability is fundamental to improving the economic landscape, and to reduce the unemployment rate. Accordingly, understanding the factors that influence cybersecurity implementation is vital.

In order to comprehend the concept of cybersecurity, it is beneficial to grasp what cyberspace is first (Thakur & Pathan, 2020). Cyberspace can be defined as a virtual world where networks of information technology infrastructure, computer systems and internet connected devices exist (Malik & Choudhury, 2019). Cybersecurity is a discipline which is all about defending the confidentiality, integrity and availability of sensitive data from hackers, government intelligence services, competitors and organised crime syndicates (Thakur & Pathan, 2020). In the same vein, Kaspersky's (2023) defines cybersecurity as "the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks" (Kaspersky, 2023). A cyberattack is a deliberate attempt by an individual or organisation, to access the network or information system of another individual or organisation, with the intention to cause harm to the individual or organisation, and to benefit from the said disruption. Cyberattacks are a daily occurrence so as the former Cisco CEO, John Chambers describes, "There are two types of companies: those that have been hacked, and those who don't yet know that they have been hacked." (Cisco, 2023). A cyber threat has the potential to cause security incident, which could lead to an actual cyber attack which can compromising an individual or organisation's information from a confidentiality, integrity, or availability perspective. Below are some of the most common cyber threats (Darem et al., 2023):

- Malware – malicious software, which is designed to damage a system, gain access to sensitive information, or disrupt the core services of the affected organisation or person.
- Distributed Denial-of-Service (DDoS) – a technique which cybercriminals use to send streams of malicious traffic to a specific organisations network. This results in the system being overloaded and leads to operational restrictions with the organisation.
- Ransomware – a form of malware which cybercriminals use to gain unauthorised access to a system, with the intention to encrypt sensitive information which the system or organisation requires or cannot afford to be in the hands of criminals. The cybercriminals then demand a ransom for the decryption code.
- Identity theft – this is when cybercriminals steal personal information via various means such as social media, email content, or paying employees of organisations for staff or customer information, with the intent to impersonate the individual, usually to commit fraudulent activity.
- Phishing / Spearphishing – a technique used by cybercriminals to elicit sensitive information from individuals or organisations via legitimate-looking means. Fraudulent emails from cybercriminals disguised as legitimate emails from your bank or a digital form on a website from a reputable company, which has been comprised.

This research, therefore, seeks to investigate the cybersecurity implementation challenges among South African SMEs. The aim is to investigate the influence that perceived ease of use, perceived usefulness, attitude, perceived behavioural control, and subjective norms has on the implementation of cybersecurity among SMEs. If found to be of value, this study can be expanded by other students or used by SMEs in Africa, and other third world countries where appropriate.

1.4 Problem Statement

Despite the increasing prevalence of cyber threats and the importance of cybersecurity for SMEs in South Africa, many SMEs continue to face challenges in implementing effective cybersecurity measures (Bada & Nurse, 2019). The lack of resources, technical expertise, and awareness of cybersecurity risks are some of the key challenges faced by SMEs in South Africa (Kirlidog et al., 2018). Communicating with businesses, particularly SMEs, can be challenging due to their operational focus and limited awareness of cybersecurity's importance (Bada & Nurse, 2019).

In a study, Mashiane and Kritzinger (2021) found that the elements belief in one's capabilities, belief regarding the consequences of actions, social influence, emotions, social and professional identity, as well as knowledge and skills, have been identified as factors that drive cybersecurity behaviour (Mashiane & Kritzinger, 2021). However, what is less clear, is how to encourage good cybersecurity practices, better hygiene, and practical ways to improve cybersecurity posture among SMEs (Iuga et al., 2016). While recent research focuses on cybersecurity within large organisations, Tam, Rao & Hall (2021) opine that there is minimal emphasis on the cybersecurity focused on SMEs in Australia or worldwide (Tam et al., 2021). Rawindaran et al. (2023) argue that the importance of SMEs being aware of and comprehending the implications of a lack of cybersecurity, cannot be overstated. This awareness and understanding can significantly impact the adoption of cybersecurity frameworks (Rawindaran et al., 2023).

This study aims to investigate the influence of perceived ease of use, perceived usefulness, attitude, perceived behavioural control, and subjective norms on the implementation of cybersecurity among SMEs in South Africa, with the goal of identifying strategies to improve cybersecurity implementation and reduce the risk of cyber threats for South African SMEs.

SMEs are a crucial part of the South African economy, therefore ensuring their sustainability is fundamental to improving the economic landscape, and to reduce the unemployment rate. Accordingly, understanding the factors that influence cybersecurity implementation is vital.

1.5 Research objective

The primary objective of this study is to investigate the cybersecurity implementation challenges among South African SMEs.

- To investigate the influence that perceived ease of use, perceived usefulness, attitude, perceived behavioural control, and subjective norms has on the implementation of cybersecurity among SMEs in South Africa

The empirical significance of this study was outlined as follows:

- To identify the factors that affect the implementation of cybersecurity among SMEs in South Africa
- To ascertain the level of agreement that SME owners attach to cybersecurity implementation challenges.
- To determine the relationship between the factors
- To determine the influence of selected demographic variables on the identifies factors.

1.6 Theoretical framework

To conceptualise the research problem, the Theory of Planned Behaviour (TPB) and the Technology Acceptance Model (TAM) will be utilised. The TPB suggests that a person's behavioural intention is based on three factors namely, the individual's attitude towards the behaviour, their perception or subjective norm, and their conviction related to their ability to perform the behaviour (Ajzen, 1985). Considered one of the most influential and commonly used theoretical models, TAM describes how individuals learn to accept information systems. This is based

on the premise that an individual's acceptance of information systems in shaped by two crucial variables namely, Perceived Usefulness (PU) and Perceived Ease of Use (PEOU) (Lee et al., 2003). The aim is to understand cybersecurity adoption and implementation through the lens of the selected theoretical models.

1.7 Rationale

This study seeks to contribute to the global conversation around an important topic in the digital era, by adding local findings to the body of international research. Cybersecurity awareness plays a major role for cybersecurity implementation among SMEs (Rawindaran et al., 2022). In an exploratory study conducted on the effect of cybersecurity awareness within SMEs in Wales, Rawindaran et al. (2022) indicate that only 30% of the 122 SME respondents sampled understood cybersecurity terminology, highlighting the low level of cybersecurity knowledge among SMEs. Many SME owners are immersed in the daily business operations and are not aware of cybersecurity threats and consequences (Bada & Nurse, 2019). Kirlidog (2018) raised that a large number of SMEs in the country lack cybersecurity awareness, and do not have the budget or skills required to secure their businesses, and they rely on government support, who themselves are lagging in the cybersecurity realm (Kirlidog et al., 2018), hence there being a critical role for academic institutions to play a pivotal role.

The study seeks to provide the impetus required to spark interest in South African academic circles, as combating cybercrime is a joint effort between government and the relevant authorities, public and private sectors, as well as academic institutions. The study aims to create awareness around the factors that influence the intention to implement cybersecurity measures, such as subjective norms, attitudes, perceived behavioural control, perceived ease of use, and perceived usefulness. By understanding these factors, SMEs can be more strategic in adopting cybersecurity practices, leading to better protection against cyber threats. Furthermore, insights from the research can assist government in the

development of targeted awareness campaigns and training programs tailored to the needs of SMEs. For example, if the study finds that perceived ease of use is a barrier, workshops could focus on demonstrating how to use specific cybersecurity tools. Based on the empirical findings, the government can also use the findings to design certification programs that encourage SMEs to prioritise cybersecurity. These programs could be more affordable and less time-consuming than existing ones, thus addressing the barriers of perceived behavioural control and ease of use.

1.8 Delimitations of the study

For this study, the following delimitations exist:

I. Cyberattacks can impact organisations of all sizes, however the focus of this paper is the SME segment.
II. The focus of this paper is cybercrime and will not investigate any other forms of crime and other forms of cyber incidents such as state operations.
III. There is a good amount of academic research on this topic globally, this paper seeks to investigate what is relevant for SMEs in South Africa, to create cybersecurity awareness, and to provide recommendations on how to circumvent the issues which are impeding the implementation of cybersecurity.

1.9 Definition of terms

Cyberspace: can be defined as a virtual world where networks of information technology infrastructure, computer systems and internet connected devices exist (Malik & Choudhury, 2019).

Cybersecurity: is a discipline which is all about protecting the confidentiality, integrity and availability of information from hackers, government intelligence services, competitors and organised crime syndicates (Thakur & Pathan, 2020).

Cyberattack: is a deliberate attempt by an individual or organisation, to access the network or information system of another individual or organisation, with the intention to cause harm to the individual or organisation, and to benefit from the said disruption (Cisco, 2023).

Cyber threats: mechanisms that cybercriminals use to compromise the confidentiality, integrity and availability of an organisation's data such as malware, distributed denial-of-service, and ransomware (Darem et al., 2023).

Cybersecurity frameworks: exist to provide organisations with the tools to assess and manage their cybersecurity risk (National Institute of Standards and Technology, 2017).

1.10 Assumptions

For this study, the following assumptions were made:

I. There is a lack of understanding with regards to cybersecurity, cyber threats and cybersecurity frameworks from a SME perspective in South Africa.
II. There is a shortage of literature on this topic in the South African context.
III. Findings from some other countries may be relevant to the local context.
IV. Findings, research limitations and areas of improvement may be further researched by academia in future.

1.11 Chapter Outline

This chapter outlined the purpose of the study i.e., to investigate the level of understanding of cybersecurity, cyber threats and cybersecurity frameworks amongst South African SME owners, and to analyse the factors which affect the implementation of cybersecurity within these SMEs. It defines the research problem, the research objectives, theoretical frameworks, and rationale for the study. Furthermore, it highlights certain delimitations, assumptions and highlights key definitions.

CHAPTER 2. LITERATURE REVIEW AND THEORETICAL FRAMEWORK

2.1 Introduction

The literature review starts by providing a historical view of cybersecurity research, which is followed by a comprehensive analysis of cyberspace, and cybersecurity as a practice. This is followed by the impact of cyber threats on SMEs, looking at the most common attack vectors. The literature review also touches on cybersecurity frameworks, with a focus on the NIST CSF and the King IV report. The literature review also provides insights into the theoretical lens of the study, namely the Theory of Planned Behaviour (TPB) and the Technology Acceptance Model (TAM) and concludes with the conceptual framework.

2.2 Trend in cybersecurity research

The growth in internet adoption, which has led to an upsurge in cloud and digital services, has transformed the way individuals and businesses operate (Yudhiyati et al., 2021). This increase in the use digital technologies has brought new security concerns, as the rapid rate of technological advancement has not been accompanied by similar advancement of the security measures required to protect businesses against cybersecurity threats (Saleem et al., 2017). Although large organisations have been the target of cybercriminals in the past, the tide is shifting with a visible rise in the number of SMEs who have experienced cyber-related attacks in recent years (Yudhiyati et al., 2021). Many SMEs are vulnerable to cyberattacks due to limited funding dedicated to cybersecurity, a scarcity of skilled cybersecurity employees, as well as an underappreciation of cybersecurity threats (Rahman & Lackey, 2013).

Although there is a plethora of literature on cybersecurity concepts, tools, and frameworks globally, there is inadequate literature on the factors that impact

cybersecurity implementation. In the South African context, cybersecurity literature is limited. An examination of academic journals and reports from credible databases such as Emerald, Sage, ScienceDirect, Google Scholar and Sabinet, to name a few, served as the basis of this paper. Results across the databases were consistent. For example, a search for “factors that affect cybersecurity implementation among SMEs” from the year 2019 to 2023, returned 57 results globally. On Sabinet Online, a database of South African journals, for the keywords “cybersecurity” and “SME” for the same period, returned 11 results. When searching “factors that affect cybersecurity implementation among SMEs” from 2019 to 2023, only 2 results were found. A few of the articles make mention of some of the reasons that cybersecurity efforts fail within SMEs, however there is limited literature on this topic. Therefore, the articles that align to some extent to the topic will be reviewed in the introduction, thereafter articles linked to cyberspace, cybercrime, cybersecurity, and cybersecurity frameworks will be unpacked.

Hasani, Rezania, Levallet, O’Reilly & Mohammadi (2023) investigated the adoption of privacy-enhancing technologies, and their effect on the financial performance of SMEs in Canada. The Technology-Organisation-Environment (TOE) model underpinned the research, incorporating other aspects such as organisational size, industry, and management readiness as possible variables that influence the adoption of privacy-enhancing technologies. This study found that readiness on the managerial, technological, environmental, and organisational levels positively influences the intention to adopt privacy-enhancing technologies, and that there was a positive correlation was between the intention to adopt privacy-enhancing technologies and organisation’s financial performance (Hasani et al., 2023). While the study by Hasani et al. (2023) makes important contributions to understanding the adoption of privacy-enhancing technologies in SMEs, it is essential to recognise its limitations and potential biases. The study by highlights several key limitations, including potential issues with sample size, diversity, and the use of a cross-sectional design, which may limit the generalizability and causal interpretations of the findings. It also identifies

potential biases, such as selection bias, country bias, and industry-specific bias, which could skew the results. Furthermore, the analysis points out gaps in the literature that the study only partially addresses, such as the need to explore industry-specific factors, external influences like regulations, and the long-term financial impact of adopting privacy-enhancing technologies in SMEs.

A study focused on the implementation of cybersecurity laws rather than cybersecurity frameworks in developing countries, was conducted by Bokhari (2023), in which responses from managers from the banking and IT sectors in Pakistan were analysed. The study revealed that the greatest impediment to the implementation of cybersecurity laws and regulations has been the rifeness of corruption. Furthermore, various elements including discrimination, unethical behaviour, skill, uncertainty, and public trust exerted a substantial impact on the implementation of cybersecurity legislation in Pakistan (Bokhari, 2023). The study offers good insights into the challenges of implementing cybersecurity laws in Pakistan, particularly the impact of corruption, but it has several limitations. The focus on the banking and IT sectors may not capture the broader spectrum of challenges across different industries, and the study's findings might not be generalisable to other developing countries facing different issues. Potential biases, such as selection bias and underreporting due to the sensitive nature of the topics, may also affect the results. Additionally, the study does not explore long-term impacts or broader governance issues, leaving gaps that future research could address through comparative and longitudinal analyses

Looking at cybersecurity governance from a South African perspective, Sutherland (2017) opines that cybersecurity regulation, government management, interactions with society and businesses, and the availability of skilled labour, South Africa falls behind more developed economies. Delays have resulted in a shortage of knowledge and insights gained from countries that have progressed more rapidly, particularly regarding policy refinements and implementation. Parliament has refrained from exerting pressure on the government to act more promptly or investigating potential instances of power

abuse that violate human rights (Sutherland, 2017). The study critically examines the shortcomings in South Africa's cybersecurity governance, emphasising delays in regulation, government inaction, and a shortage of skilled labour, however, the study does have limitations such as a narrow focus on government failures without adequately exploring the roles of the private sector or international cooperation. Potential political bias and the lack of comparative analysis with other developing countries also limit the study's broader applicability. Addressing these gaps through deeper analysis and international perspectives could provide a more comprehensive understanding of how South Africa can improve its cybersecurity governance.

A paper by Choejey, Murray & Fung (2016), investigating the critical success factors for the implementation of cybersecurity in Bhutanese government organisations, indicated that the effective execution of cybersecurity measures is contingent upon a comprehensive comprehension of the cyber threats and obstacles that the information assets of the organisation face. Identifying a responsible and committed staff to lead and direct cybersecurity initiatives is also crucial. Moreover, for management to target, prioritise, and implement cybersecurity activities, it is crucial to identify the critical areas. The survey results indicate that education, training, and awareness are the top cybersecurity success factors for government organisations. In addition, the security procedures, policies, and standards, funding and resources for cybersecurity, support from senior management, and cybersecurity compliance and auditing are critical factors (Choejey et al., 2016). From a limitations perspective, its focus on Bhutan's specific context may limit the generalisability of its findings to other regions or sectors. Potential biases, such as selection and cultural biases, may influence the results, and the study's reliance on survey data could lead to overemphasis on certain factors. Additionally, the study does not fully address the impact of external threats or the long-term effectiveness of these success factors, leaving gaps that future research could explore through comparative and longitudinal analyses.

A paper by Saleem, Adebisi, Ande & Hammoudeh (2017) provided an overview of the substantial cybersecurity concerns that have an impact on various sectors of digital technology. The analysis centred around current trends in cybersecurity and the consequences of intrusions on SMEs, encompassing simple computers, IoT devices, smart automobiles, and even conventional corporate servers. The study also assisted to bring about awareness on the topic for non-technical researchers, experts and practitioners (Saleem et al., 2017). The prevalence of digital attacks targeting SMEs has reached a level of frequency that it is now considered common due to; 1) the threat of cybersecurity is often underestimated by small enterprises; 2) SMEs have limited financial resources to effectively implement security measures; 3) there is a severe shortage of skilled security personnel; and 4) the exorbitant expense of security solutions and employee security awareness training further discourages some SMEs from deploying effective solutions (Ghafir et al., 2018). The study's lack of empirical data, broad scope, and potential generalisation bias limit its depth and applicability. It highlights significant barriers for SMEs, such as high costs and limited resources, but does not provide a detailed cost-benefit analysis or practical recommendations. Additionally, the study does not address how cybersecurity threats and strategies evolve over time. Future research could benefit from empirical evidence, actionable strategies, and a longitudinal approach to better understand and address cybersecurity challenges for SMEs.

Boritz, Ge & Patterson (2022) analysed the variables that are linked to employee susceptibility to phishing attacks. Scepticism, suspicion of hostility, and interpersonal trust are the three dimensions of suspicion that were assessed. Additionally, three cognitive traits were evaluated; these being risk-taking propensity, cognitive control, and social cognition (Boritz et al., 2022). The narrow focus on specific traits may overlook other factors influencing phishing vulnerability, and potential biases in self-reported data and measurement could affect accuracy. The study does not explore broader contextual factors or provide practical interventions. Future research could address these gaps by

incorporating a wider range of variables, examining changes over time, and developing strategies to mitigate phishing risks.

Gonzalez-Granadillo, Gonzalez-Zarzosa, & Diaz (2021) unpacked Security Information and Event Management (SIEM), which is regarded as a powerful and widely used tool to avoid, detect and respond against cyberattacks. A comprehensive examination of the functionalities and attributes of existing SIEMs were conducted, including an examination of exogenous variables (political, economic, societal) that may have an impact on forthcoming SIEMs, and a summary of SIEM solutions in critical infrastructures was presented to illustrate potential applications of these instruments (González-Granadillo et al., 2021). The study provides good insights SIEM functionality, however the study's scope may be too broad, lacking in-depth analysis of specific SIEM solutions and their real-world performance. Potential biases include selection bias towards more prominent solutions and possibly subjective interpretations of the impact of external variables. Additionally, the study does not address integration challenges, usability issues, or future advancements in SIEM technology. Future research could benefit from a focus on empirical performance evaluations, practical integration strategies, and emerging trends in SIEM systems.

Bada & Nurse (2019) proposed a high-level cybersecurity education and awareness program for use by governments, NGOs, and other organisations when targeting SMEs at the city level, in order to draw attention to the security challenges faced by SMEs (Bada & Nurse, 2019). While their proposal contributes to the discourse on improving cybersecurity awareness, several limitations, potential biases, and gaps need to be critically analysed. The study lacks empirical validation and practical implementation details. The broad, high-level recommendations may not address the specific needs or constraints of different SMEs and might be influenced by contextual biases. Additionally, the study does not explore the challenges of program deployment or assess its potential impact on improving SME cybersecurity practices. Future research

should focus on practical implementation strategies, impact evaluations, and customized programs tailored to the diverse needs of SMEs.

In another paper focused on awareness, Rawindaran et al (2022) explored how SMEs in Wales are effectively addressing cybercrime and safeguarding their data while conducting routine online activities to combat cyber threats (Rawindaran et al., 2022). While this research sheds light on practical approaches and strategies used by SMEs, limitations, potential biases, and gaps should be considered. The study's focus on a specific region may limit the generalisability of its findings to other areas or contexts. There may be selection bias if it highlights practices of more successful SMEs and reporting bias if participants present an overly positive view of their cybersecurity measures. The research might also lack detailed insights into specific strategies and tools used and may not address how SMEs adapt to emerging threats or the long-term effectiveness of their practices. Future studies could benefit from a broader comparative analysis, and a deeper exploration of specific cybersecurity measures.

Another study, underpinned by the Protection Motivation Theory, investigated the impact of cybersecurity policy mindfulness on the improvement of reactive capabilities for supply chain cyber resilience (Wong et al., 2022). While the study offers important insights into the role of policy mindfulness, several limitations, and potential biases warrant examination. The study may be limited by its theoretical focus on only reactive capabilities, potentially overlooking proactive measures and other relevant factors. Potential biases include selection and reporting biases, which could affect the accuracy of findings. Additionally, the study might not fully address how its results apply across different industries or over time. Future research could benefit from a more comprehensive approach that integrates both proactive and reactive strategies, explores different theoretical frameworks, and assesses long-term impacts.

A study by Alawida et al. (2022) investigates the increase in cyber-crime during the COVID-19 pandemic, detailing various types of cyber-attacks and their evolution over time. Initially, attacks were rare but became frequent, with reports

of multiple attacks on some days. The study identifies fifteen common types of cyber-attacks (Figure 1 below) and examines their patterns and impact. A qualitative approach and multi-criteria decision-making technique were used to rank the severity of different cybersecurity issues. Data from a global survey conducted from March 2020 to December 2021 revealed that hacking attacks were the most common, followed by spam emails, malicious domains, and others (Alawida et al., 2022). The study suggests that governments and organisations must remain resilient and innovate in cybersecurity to address current and future threats effectively. Despite its valuable contributions to understanding pandemic-related cyber threats and offering practical recommendations for enhancing cybersecurity, the study has limitations including its temporal scope, potential biases in data collection and reporting, and reliance on qualitative methods, which may affect the generalizability of its findings

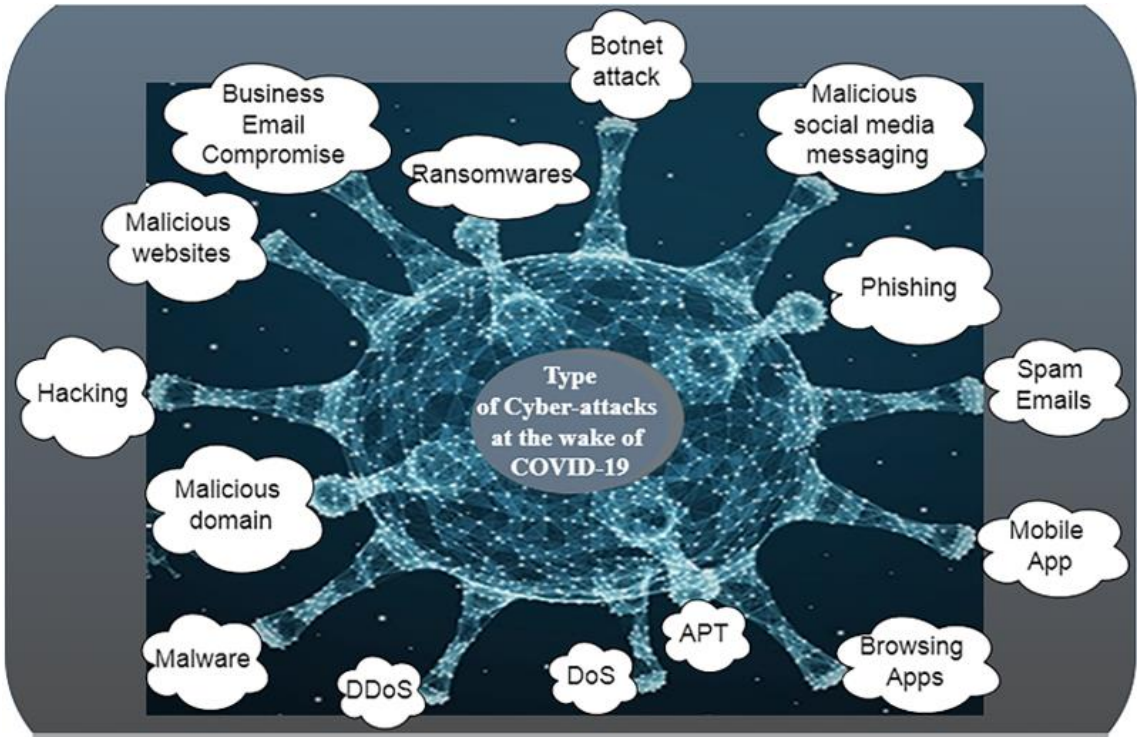


Figure 1: Main Cybersecurity Threats in the wake of COVID-19 (Alawida et al., 2022)

In another post-COVID study, Kumar et al. (2022) explore how the COVID-19 pandemic has shifted the focus within the cybersecurity field. By analysing over twenty thousand documents using machine learning, the study examines changes in key themes from 2010 to 2021. It finds that while pre-pandemic discussions centred on topics like cyber-threats, privacy policy, and blockchain, post-pandemic research has increasingly focused on issues such as privacy in healthcare, cyber insurance, and supply chain risks. Despite these shifts, topics like malware and control system security remain relevant. The study highlights the evolving nature of cybersecurity and the need for targeted interventions based on emerging trends (Kumar et al., 2022). It is important to also consider potential biases and limitations inherent in the study. The study analyses over twenty thousand documents but does not specify the exact proportion of scholarly versus non-scholarly sources. The inclusion of non-peer-reviewed literature may introduce variability in the quality and reliability of the data, potentially affecting the accuracy of the findings. Additionally, the use of Latent Dirichlet Allocation (LDA) for topic modelling, while useful, may not fully capture the nuanced context of cybersecurity issues. LDA can sometimes oversimplify complex themes or misclassify documents, potentially leading to skewed results.

Finally, Saleous et al. (2022) investigate the heightened cybersecurity risks during the COVID-19 pandemic, detailing how cybercriminals exploit vulnerabilities in individuals, businesses, and systems amid the crisis. It identifies various cyber threats, attack vectors, and surfaces, and reviews the implications of these threats based on recent attacks. The study underscores the importance of global cooperation to mitigate these risks and provides recommendations for professionals and researchers, aiming to advance research and responses in this evolving field (Saleous et al., 2023). The study's focus on recent literature may limit its scope, and potential biases could affect the representation of cybersecurity issues. The study may exhibit selection bias if it primarily draws from certain sources or types of literature, such as those from specific regions. There could be a reporting bias where the study focuses on more dramatic or high-profile cyber incidents, potentially overshadowing less visible but still

significant threats. It does however address important gaps by highlighting the evolving threat landscape and the necessity for coordinated international efforts.

The rest of the chapter will review concepts of cybercrime and cyberspace, as the underlying context within which cybersecurity exists, then a review of cybersecurity as a practice to combat cybercrime, which is followed by a comprehensive review of the various cyber threats that cybercriminals use as their attack vectors, followed by an evaluation of some of the available cybersecurity frameworks, a review of the theoretical models which underpin the study, namely the Technology Acceptance Model and the Theory of Planned Behaviour, and finally, the proposed conceptual model is explained.

2.3 Understanding cybercrime and cyberspace

2.3.1 Cybercrime

Cybercrime has become rampant among various organisations (Kurpjuhn, 2015). Cybercrime frequently involves unauthorised access to information systems, such as devices, applications, or the internet. Sussman and Heuston coined the term 'cybercrime' in 1995 (Sarmah et al., 2017). Given the trend of increasing cyber-attacks on people and the economy, it is becoming vital to comprehend the backgrounds to a users' security perceptions, and resulting behaviour (Weickert et al., 2023). In the literature on cybersecurity, methods for addressing this concern include investigating the human element of security through notions such as user behavioural compliance (Bélanger et al., 2017), the aim and impetus to follow security procedure (Egelman & Peer, 2015; Son, 2011), as well as security awareness (Siponen, 2000).

In order to encourage individuals to consider cybersecurity policy seriously, researchers bank on concepts from psychology and behavioural economics, such as the Protection Motivation Theory (Rogers & Prentice-Dunn, 1997) and the Nudge Theory (Enisa, 2018; Thaler & Sunstein, 2008). Rogers and Prentice-

Dunn (1997) describe the Protection Motivation Theory (PMT) as a psychological paradigm that explains how individuals perceive threats and respond to them. The theory focuses on identifying the factors that motivate individuals to protect themselves and take preventive measures. Overall, the article emphasises the role of perceived vulnerability, perceived severity, response efficacy, self-efficacy, and response costs in shaping individuals' assessments and subsequent behaviour. Thaler and Sunstein (2008) discuss the Nudge Theory, which proposes that individuals can be influenced to make better decisions and enhance their decision-making using subtle, non-coercive interventions known as "nudges." The theory focuses on the design of choice architectures that steer individuals toward desirable outcomes without limiting their freedom of choice. The article argues that the Nudge Theory offers a novel perspective on behaviour modification by utilizing human psychology and choice architecture to promote improved decision-making.

As a result of the surge in cybercrime, SMEs are vulnerable to similar risks as large organisations, but often lack the necessary resources to mitigate the associated risks (Kurpjuhn, 2015). Paulsen et al. (2016) proposes that one of the potential reasons for the increase in targeting of SMEs is their relatively weaker cybersecurity programs, which are due to limited cybersecurity education and awareness, as well as insufficient resources such as dedicated cybersecurity budgets, skills, and the necessary infrastructure, in contrast to large organisations (Paulsen & Toth, 2016). Baba and Nurse (2019) highlight that SME owners' immersion in daily business operations could also contribute to cybersecurity struggles. In an exploratory study conducted on the impact of cybersecurity awareness on SMEs in Wales, Rawindaran et al. (2022) reported that only 30% of the 122 SME respondents sampled understood cybersecurity terminology, highlighting the low level of cybersecurity knowledge among SMEs. From an awareness and education perspective, there is a need for SMEs to understand concepts such as cyberspace, cybersecurity, cyber threats, and cybersecurity frameworks, which include risk mitigation strategies.

To comprehend cybersecurity, it is essential to understand the concept of cyberspace, which refers to the virtual world encompassing information technology infrastructure, computer systems, and internet-connected devices (Clemente, 2015; HM Government, 2016). Cybersecurity is the discipline focused on safeguarding information's confidentiality, integrity, and availability from malicious actors such as hackers, government intelligence services, competitors, and organized crime syndicates (Clemente, 2015; Kaspersky). Cyberattacks are intentional actions aimed at gaining unauthorized access to another individual or organisation’s network or information system, causing harm and seeking personal gain (Cisco, 2023). These attacks compromise information from the perspectives of confidentiality, integrity, and availability. Cyber threats are the tactics employed by cybercriminals to compromise the confidentiality, integrity, and availability of an organisation’s information (Donaldson et al., 2018).

2.3.2 Cyberspace

Cybersecurity cannot be viewed in isolation; it must be understood within the context of cyberspace (Wang et al., 2023). Human activities have undergone a digital transition that has moved many of them into cyberspace, where people can work together and at the very least rethink the role that distance plays (Cairnoss & Cairncross, 2001). People can communicate from anywhere without incurring travel expenses in online social networking sites like Facebook or Twitter, which removes the restrictions of space and time from interactions between them. Chen et al (2023) define cyberspace as decentralized human activities, social interactions, and application services in the information space that are transmitted by sensors and internet communication channels and supported by cyberinfrastructure. In a similar fashion, Kim et al (2023) propose that cyberspace can be defined as a global, interdependent information system infrastructure which consists of the internet and networks.

Cyberspace is divided into three layers namely, the Physical layer, Logical layer and the Persona layer (Kim et al., 2023). Kim et al (2023) unpack the layers as follows:

1. Physical layer – the physical network components such as computers, servers, and routers.
2. Logical layer – logical components that exist between network nodes such as operating systems and applications.
3. Persona layer – the information layer containing information about users such as email information or social media accounts.

The UK National Cybersecurity Strategy (2016) adds a fourth layer called the Top layer. The Top layer refers to the people or robots or technologies such artificial intelligence who manipulate information, and who are responsible for designing the Physical and Logical layers. These interrelated layers capture crucial characteristics of cyberspace. Cyberattacks can occur at any layer, including physical damage of components, logical element compromise, information corruption, and human corruption, therefore cyber defence must be based off a thorough understanding of all these layers (HM Government, 2016).

The layers mentioned above, have three characteristics – connectivity, speed, and storage. These characteristics enable both positive and negative aspects of the digital environment (HM Government, 2016). 68% of the world is connected to the internet via mobile devices, laptops, and tablets. Furthermore, there are billions of connected things via the Internet of Things (Internet World Stats, 2021). The rapid increase in connectivity enables digital transformation, new ways of work and communication and nullifies distance, as well as brings greater risk and opportunity for cybercriminals (Brownstein et al., 2008). With the advancement of technology and computer hardware, the possibility to place more transistors on a chip means greater speed, which also the means more opportunity in the digital world. Unfortunately, this also means more opportunity for cybercriminals. Storage involves the capacity and performance capability of a device. Storage is

a valuable asset to a cybercriminal who intends to store large amount of data (HM Government, 2016).

2.4 Cybersecurity

The technological revolution has led to a fundamentally different way of working, living, and interacting. As a result, organisations need to enhance their capabilities to keep up with the changing demands, and to provide the customer experience needed in this new digital era. In doing do, they also need to ensure that they secure their operations and protect themselves from cybercriminals. Therefore, cybersecurity needs to be a priority for business and society at large (Jurgens, 2022). Although people have grown incredibly reliant on computer networks in their daily lives as well as their work lives, technology and digital transformation is moving faster than the rate within which cybersecurity can improve. Cybersecurity mishaps are common worldwide and impact people, businesses, and governments. Nowadays, maintaining a good cybersecurity posture is extremely difficult due to the growth of hacker attack methods (Wang et al., 2023).

Furthermore, connectivity, speed, and storage, creates both opportunity and threats in cyberspace. Cybersecurity is the practice of protecting internet-connected systems and their data, from unauthorised use (HM Government, 2016). “Cybersecurity is defined as the totality of the processes, governance, management, tools, policies and controls that are deployed to secure a digital environment, which includes the assets (i.e. information assets and cyber assets), entities (such as end users, organisations, governments, societies, machines and software) and interactions (enabled by IT infrastructure, communications/networks, systems and devices), by eliminating, reducing or mitigating the risks of unauthorized access and/or control, disruption, damage or other cyberattacks” (Azmi et al., 2018; ISACA, 2013; Kissel, 2013).

Cybersecurity is a set of tools and processes, intended to protect the cyber environment of an individual or organisation. It is a set of technologies, techniques and procedures used to prevent unauthorised access to systems and data, to protect the confidentiality, integrity, and availability of data. Increasing reliance on computer systems, such as mobile devices, televisions, and the myriads of tiny devices that make up the Internet of Things, has increased the field's significance. (Seemma et al., 2018). SMEs also face several security-related obstacles due to inadequate budgets, limited resources, and insufficient cybersecurity skills. As there are no permanent solutions available for the problem at hand, the rapid expansion of technologies also makes cybersecurity more difficult. Although the industry is actively fighting and presenting numerous frameworks and technologies to secure an organisation’s information security, the solutions are only seemingly temporary in nature. However, improved security awareness, knowledge and strategies can help businesses protect intellectual property and trade secrets while minimising financial and reputational loss (Goutam, 2015).

In 2017, the Department of Telecommunications and Postal Services (DTPS) and the Council for Scientific and Industrial Research (CSIR) conducted a Cybersecurity Readiness Survey to assess the security status across key sectors in the country. At the time, cyber-attacks against information infrastructure and internet services became increasingly common, placing significant responsibility on governments and organisations to protect citizens. These attacks often resulted in lost revenue, service disruptions, and damage to a country's reputation. South Africa, as a developing nation, faced a growing threat from cyber-attacks, particularly as more services transitioned to digital platforms. The limited cyber knowledge in developing areas made it challenging to defend against common attacks like phishing, malware, and identity theft. Therefore, the report aimed to address the lack of published research on current cybersecurity strategies, governance, standards, awareness, risk assessments, incident management, and business continuity. The findings are intended to help organisations better understand the importance of their data and improve their

preparedness for cyber-attacks in order to improve the overall cybersecurity situation in the country (Veerasamy, 2017).

In 2020, Accenture released Insight into the Cyberthreat Landscape in South Africa, where malware attacks increased by 22% between January and March 2019, which worked out to 577 attempted attacks every hour. During that period, South Africa saw a 100% increase in mobile banking fraud cases (Mcanyana et al., 2020). Cybercriminals may believe that the South African population and businesses have lower cyber defences as compared to developed countries, due to a general lack of investment in cybersecurity, poor awareness about cyber threats, and the fact that the country has been slow to adopt appropriate cybersecurity legislation (Mcanyana et al., 2020).

In 2023, South Africa experienced a 22% rise in cyber attacks, particularly affecting small businesses, according to the South African Banking Risk Information Centre (SABRIC). This highlights the critical need for robust cybersecurity measures as threats continue to evolve. The current cyber threat landscape is marked by sophisticated attacks targeting individuals, businesses, and governments, with ransomware, phishing, social engineering, and digitally enabled fraud being the most common. The increasing use of AI technologies by cybercriminals has further heightened the complexity of these attacks (Seacom, 2024)

2.5 Impact of cyber threats on SMEs

A cyberthreat or cyberattack is nothing more than a means of breaching the barriers to a victim's network and compromising computer functionality or gaining unauthorized access to a victim's computer (Dasgupta et al., 2022). Cyberattacks compromise the confidentiality, integrity, and availability of data and computer systems. These include unauthorized access to computer systems, illegal interception of data transmissions, data interference (damaging, deletion, deterioration, alteration, or suppression of data), system interference (the

unauthorised obstructing of the proper operation of a computer or system), forgery, fraud, and identity theft (Mphatheni & Maluleke, 2022).

SMEs constitute the majority of enterprises worldwide (Alharbi et al., 2021). However, they face challenges in comprehending the potential consequences of cybersecurity threats on their businesses, and the potential harm they might inflict on their assets (Alharbi et al., 2021). The World Bank estimates that SMEs will generate 70% of the total job growth by 2030 and account for over 50% of global employment (Ali & Wanasilpb, 2022). In emerging economies, SMEs contribute about 40% of the gross domestic product (GDP). The rise in cyber-attacks targeting SMEs is concerning, given the significance of SMEs (Ali & Wanasilpb, 2022).

The top cyber threats for an emerging economy like South Korea are as follows; malware, GPS interruption, hacking, DDoS and smartphone hacking (Jung et al., 2020). The following sections will detail the different types of cyber threats out there.

2.5.1 Types of cyber threats

Below are some of the most common cyber threats according to Donaldson et al. (Donaldson et al., 2018):

- Malware – malicious software, which is designed to damage a system, gain access to sensitive information, or disrupt the core services of the affected organisation or person.

- Distributed Denial-of-Service (DDoS) – a technique which cybercriminals use to send streams of malicious traffic to a specific organisations network. This results in the system being overloaded and leads to operational restrictions with the organisation.

- Ransomware – a form of malware which cybercriminals use to gain unauthorised access to a system, with the intention to encrypt sensitive

information which the system or organisation requires or cannot afford to be in the hands of criminals. The cybercriminals then demand a ransom for the decryption code.

- Identity theft – this is when cybercriminals steal personal information via various means such as social media, email content, or paying employees of organisations for staff or customer information, with the intent to impersonate the individual, usually to commit fraudulent activity.

- Phishing / Spearphishing – a technique used by cybercriminals to elicit sensitive information from individuals or organisations via legitimate-looking means. Fraudulent emails from cybercriminals disguised as legitimate emails from your bank or a digital form on a website from a reputable company, which have been comprised.

There are various ways, as displayed in figure 1 (cyberattack taxonomy), in which cybercriminals can try to breach the defences of computer systems (Al-Enezi et al., 2014). Al-Enezi et al. (2014) also provide insights on cyberattacks, which formed the basis of Dasgupta et al. (2022) paper on “Machine learning in cybersecurity: a comprehensive survey” (Al-Enezi et al., 2014; Dasgupta et al., 2022).

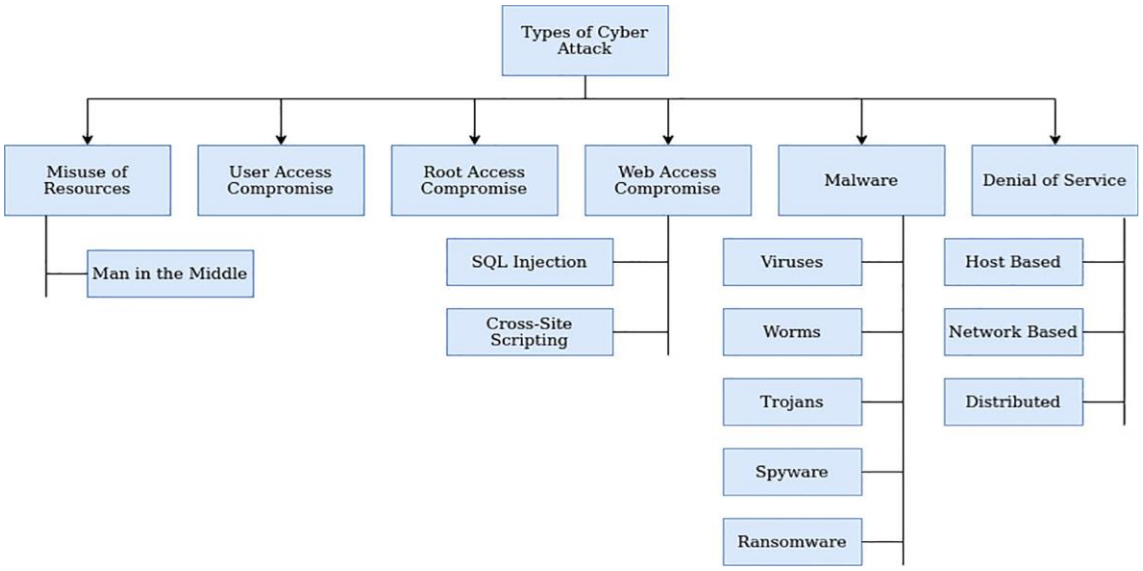


Figure 1: The Cyberattack Taxonomy (Dasgupta et al., 2022)

- Misuse of resources attack – unconsciously oblivious employees from a business can cause security weaknesses, thereby granting access to attackers to the organisation's information. An employee, with no malicious intent, could open an email or make a payment, which allows attackers to cause massive damage to the organisation (Dasgupta et al., 2022).
- User access compromise – the compromise of a user's information, like a username and password, is a common occurrence. Surfing computer systems to obtain poorly encrypted passwords, social engineering assaults to access a password folder, calculated guessing and dictionary attack are popular methods for obtaining the personal credentials of a user. Phishing and spearphishing are common methods of infiltrating sensitive information. A popular method employed is the use of a malicious email attachment, containing a call-to-action to an authentic website, that subsequently downloads malware or asks for login credentials (Dasgupta et al., 2022).
- Root access compromise – like the above, but with higher risk. In this instance, attackers are able to penetrate an administrator's account, which by its nature, has more privileges than other accounts on the system (Dasgupta et al., 2022).
- Web access compromise – an attack via Structured Query Language (SQL) injection or malicious script, to take advantage of a poorly protected website (Dasgupta et al., 2022).
- Malware attack – malware, which is an abbreviation for malicious software, in simple terms, is an unwelcome software application. Cybercriminals have used malware over the years to accomplish cybercrime objectives, such as bringing systems to a halt, and gaining access to unauthorised data. There are number numerous types of malware attacks (Dasgupta et al., 2022):

a) Viruses: a virus is a fragment of malicious code that is carried by files and corrupts records on the targeted system, as well of on the rest of the network (Dasgupta et al., 2022).

b) Worms: worms have a distinct propagation mechanism than viruses. Unlike viruses, worms can replicate without a host computer. Self-replicating worms typically arrive as email attachments (Dasgupta et al., 2022).

c) Trojan: A trojan is entirely distinct from viruses and worms in terms of its intent. Utilizing social engineering techniques, attackers delude users into installing a trojan on their computer (Dasgupta et al., 2022).

d) Spyware: rather than negatively impacting the user immediately, spyware sits in the background and gathers sensitive data like user credentials, without the user knowing (Dasgupta et al., 2022).

e) Ransomware: this malware not only negatively impacts the functioning of a system, but it also initiates the request for a ransom from the target. Typically, ransomware is conducted via trojans (Dasgupta et al., 2022).

- Denial of service (DOS) – completely destabilising the operations of a system is the primary objective of this type of attack. There are three primary categories of DoS attacks – 1) host-based attacks are where the host's machine is targeted, which then send thousands of requests to the network, thereby bringing it to a grinding halt, 2) network-based attacks where the attackers target the network directly but achieve a similar outcome, and 3) Distributed DOS is where the attackers target both the host and the network (Dasgupta et al., 2022).

In a report from Cyberinsights, Wirth (2019) shares another form of attack. Crypto jacking is an attack that mines cryptocurrency using stolen processing power, cloud central processing unit cycles, or network bandwidth. Mining cryptocurrency is not illegal in and of itself; it is the process of conducting the cryptographic calculation underlying a blockchain transaction. However, doing so by stealing someone else's computing capacity is illegal and can result in system

performance degradation, overheating, and even equipment destruction (Wirth, 2019).

2.6 Cybersecurity frameworks

Cybersecurity frameworks exist to provide organisations with the tools to understand and manage their current cybersecurity posture, and to ensure interventions are in place to reduce its risks associated to cybersecurity (National Institute of Standards and Technology, 2017). Cybersecurity frameworks provide a detailed, organised record of all the crucial fundamentals of a business's cybersecurity programme (CTO, 2015).

There are numerous cybersecurity standards available to a business. From a South African perspective, the King IV Report on Corporate Governance underscores the importance of incorporating cybersecurity into an organisation's overall governance and risk management strategies. It highlights the board's responsibility to oversee cybersecurity as a critical risk, ensuring that appropriate measures are in place to protect data and manage evolving threats. The report also emphasises ethical considerations in technology use, transparency in reporting cybersecurity practices to stakeholders, and the need for continuous improvement in cybersecurity measures to adapt to new risks (Africa, 2016). Globally, there are a few common standards in place. To name a few – the International Standardization Organisation (ISO) 27000 series, Information Technology Infrastructure Library (ITIL), Control Objectives for Information Technologies (COBIT), and the National Institute of Standards and Technology Cybersecurity framework (NIST CSF) (Baker, 2012). The NIST CSF and ISO 27000 frameworks are the two most common standards utilised globally (Antunes et al., 2022). They provide a set standards that are implemented by specialised tools designed to capture and analyse enterprise-level information security auditing (National Institute of Standards and Technology, 2017).

A common issue raised with cybersecurity frameworks is that they do not have clear implementation guidelines (National Institute of Standards and Technology, 2017). It must be noted that the auditing requirements of SMEs differ from those of large organisations, and cannot be applied to a SME's auditing process (Antunes et al., 2022).

Furthermore, whilst an ISO information security standard provides organisations with sets of recommendations regarding what they could do to enhance information security, it frequently lacks concepts that describe when and where the recommendations would be applicable. Additionally, ISO standards typically do not define how the recommendations should be implemented. While certification programs based on ISO standards have been implemented, one notable drawback of the certification approach is that ISO compliance does not guarantee a strong cybersecurity strategy. The ISO 27000 series also has a limited scope, focusing primarily on information security rather than the broader domain of cybersecurity (Dedeke & Masterson, 2019). Consequently, the rest of this section will focus on the NIST CSF.

2.6.1 NIST CSF Framework

The NIST CSF comprises of five concurrent and continuous functions at its core that can be utilised by any organisation regardless of size, level of cybersecurity risk and sophistication. The following include the five steps of the NIST framework (National Institute of Standards and Technology, 2018):

(1) Identify: Comprehend the cybersecurity risk to systems, assets, data, and capabilities.

(2) Protect: This includes implementing appropriate safeguards to secure critical infrastructure services.

(3) Detect: This entails implementing the proper activities to identify the occurrence of cybersecurity incidents.

(4) Respond: It includes the implementation of measures to mitigate the impact of detected cybersecurity incidents.

(5) Recover: This involves implementing the appropriate activities and strategies to ensure rapid restoration of capabilities or services that have been compromised by a cybersecurity incident.

Table 1: NIST functions and categories (National Institute of Standards and Technology, 2018)

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Table 1 unpacks the NIST CSF functions into their various categories (and can be further dissected in sub-categories (National Institute of Standards and Technology, 2018). To explain how the framework operates consider the following example – if an organisation is concerned about its incident response

plan, it can examine the "Respond" function. The Respond function consists of five categories: (1) Response Planning, (2) Communication, (3) Analysis, (4) Mitigation, and (5) Enhancements. Each of these categories is subdivided into numerous subcategories of cybersecurity operations. For instance, the "Response Planning" category contains one subcategory (i.e., "Response plan is executed during or after an event"), whereas the "Improvements" category contains two subcategories (i.e., "Response plans incorporate lessons learned" and "Response strategies are updated"). Each subcategory then references relevant resources which are industry best practices, to cater for the specific requirement (Shen, 2014).

Although the literature advocates for the NIST as a suitable and flexible framework, a few concerns regarding its usage are highlighted. For example, a study by Ravindranath (2017) found that 46% of 250 respondents indicated that the NIST CSF was too time consuming while 45% of these respondents believed it is too complex. In addition, implementing NIST can be costly. Given the reports on the time and resources necessary to implement NIST, it is essential to develop cybersecurity solutions that can be adopted based on priorities and resource availability (Goel et al., 2020).

The National Institute of Standards and Technology, in conjunction with government and the private sector, created a tool to protect United States (U.S.) organisations (Shen, 2014). The issue is that many U.S. organisations are not applying the NIST framework into their operations (Bonnema, 2018; Brown, 2016). In this light, a study by Yvon (2020), on the factors which hinder SMEs from executing the NIST cybersecurity framework, the following factors were highlighted:

- Complexity – the overall design of the framework is seen as comprehensive and strategic, but complex for SMEs to apply in their business environment.
- Lack of skillset – the study identified a difficulty in recruiting suitably qualified candidates with the cybersecurity skills, lack of cybersecurity

proficiency withing the leadership team, and the lack of a devoted cybersecurity team.

- Expensive – cost was idented as another limiting factor. Three sub-factors emerged as 1) the fear of not knowing the costs involved in cybersecurity, 2) apportioning cybersecurity costs from the overall budget of the organisation, 3) gaining an appreciation of the costs versus the risks associated.
- Not a required regulatory requirement – the fact that the NIST CSF is voluntary and not mandatory, hinders its implementation.
- Lack of cybersecurity knowledge – lack of awareness of cybersecurity as a practice was highlighted as another factor. Four subfactors emerged as 1) lack of understanding of whether a cybersecurity program is required or not, and when to implement, 2) uncertainty of which framework is most suitable, 3) limited understanding of where to locate relevant cybersecurity material which is for SMEs, and 4) the fear of the unknown.

2.6.2 King IV Report

The King IV Report on Corporate Governance emphasises the importance of integrating cybersecurity into an organisation's overall governance and risk management strategy (Africa, 2016). It provides the following guidance (Africa, 2016):

Board responsibility: The board is accountable for overseeing the governance of information and technology, which includes cybersecurity. This involves ensuring that cybersecurity is aligned with the organisation's overall strategy and that risks are effectively managed.

Risk management: Cybersecurity should be treated as a critical risk factor. The board must ensure that processes are in place to identify, assess, and mitigate cybersecurity risks. This includes regular monitoring and updating of cybersecurity measures to respond to evolving threats.

Data protection: The King IV Report highlights the importance of protecting personal and sensitive information. Organisations are expected to comply with relevant data protection laws and implement robust measures to safeguard data from unauthorized access or breaches.

Ethical use of technology: The report encourages ethical considerations in the use of technology, ensuring that the organisation's digital activities do not harm stakeholders or compromise the integrity of information.

Transparency and reporting: Organisations should be transparent about their cybersecurity strategies and risks. This includes clear communication with stakeholders about how cybersecurity risks are managed and what steps are being taken to protect the organisation and its data.

Continuous improvement: The report recognizes that cybersecurity is a dynamic field. Organisations are advised to continuously update their cybersecurity policies, practices, and technologies to address new and emerging threats effectively.

Overall, King IV stresses the integration of cybersecurity into the core governance framework, ensuring it is treated as a strategic priority within the organisation's broader risk management and ethical guidelines.

2.7 THEORETICAL FRAMEWORK

To conceptualise the research problem, the Theory of Planned Behaviour (TPB) and the Technology Acceptance Model (TAM) will be utilised. The TPB suggests that a person's behavioural intention is based on three factors namely, the individual's attitude towards the behaviour, their perception or subjective norm, and their conviction related to their ability to perform the behaviour (Ajzen, 1985).

Considered one of the most influential and commonly used theoretical models, TAM describes how individuals learn to accept information systems. This is based on the premise that an individual's acceptance of information systems in shaped

by two crucial variables namely, Perceived Usefulness (PU) and Perceived Ease of Use (PEOU) (Lee et al., 2003).

2.7.1 Theory of Planned Behaviour (TPB)

The TPB, which was developed by Ajzen (1991), proposes that the intention to engage in a specific behaviour is a result of three independent variables, namely the individual's attitude towards the behaviour, their perception or subjective norm, and their conviction related to their ability to perform the behaviour (Ajzen, 1991). As depicted in Figure 3, the model indicates that an individual's attitude towards the behaviour, their perception or subjective norm, and their conviction related to their ability to perform the behaviour, impacts their intention to engage in the behaviour. The stronger the intention, the better the chance that the individual would engage in the behaviour (Chipeta, 2019). TPB is the second most widely used theory in the field of cybersecurity behavioural research (Alsharida et al., 2023), and is used extensively in information security related research (Aigbefo et al., 2022; Alanazi et al., 2022; Hong & Furnell, 2022; Ma, 2022; Philip et al., 2023; Vrhovec et al., 2023).

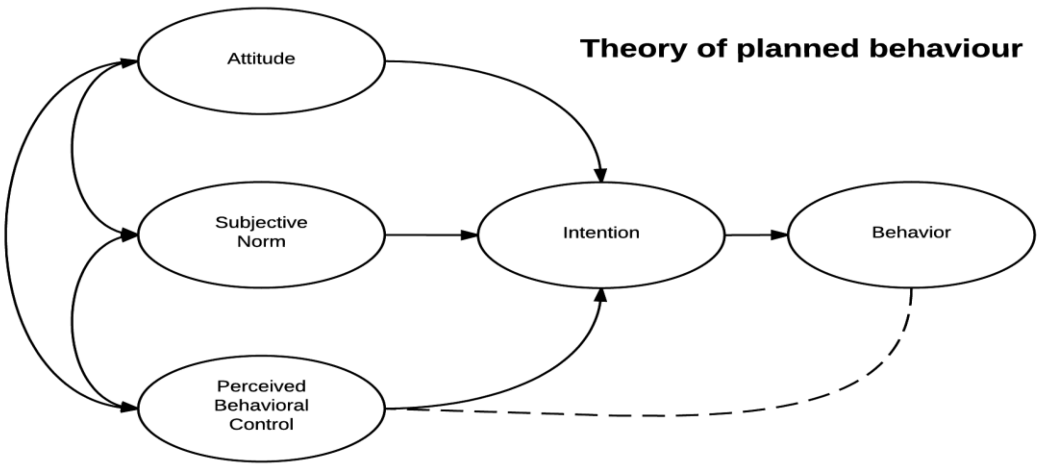


Figure 2: Theory of Planned Behaviour

Looking at the various constructs within the TPD, attitude is defined as an individual's feelings, whether negative or positive, towards performing a specific behaviour, and is guided by one's perception of whether the outcomes of the specific behaviours are desirable or not. Subjective norms are linked to the opinions of people close to the individual who is performing the behaviour, and whether they believe that the behaviour should be performed or not. Perceived behavioural control is based on the individuals perception of the level of difficulty involved in performing the behaviour (Ajzen, 1991).

Various studies have proposed that attitude (Al-Debei et al., 2013; Cheung & To, 2016; Law, 2020; Mohit et al., 2023; Song et al., 2018; Sun et al., 2017), subjective norms (Dholakia & Soltysinski, 2001; Lee & Geistfeld, 1998; Li, 2007; Nafees et al., 2021; Rahman et al., 2020; Rau et al., 2008; Todd & Benbasat, 2000), and perceived behavioural control (Bautista et al., 2022; Cheung & To, 2016; Chu et al., 2016) all play fundamental roles in impacting the intention to behave in a certain way, which then leads to actual change in behaviour. Alanazi et al. (2022) found that the propensity of young adults to participate in cybersecurity practices is directly associated with the perceived behavioural control, subjective norms, and their attitude towards cybersecurity (Alanazi et al., 2022). Aigbefo et al. (2022) agreed that attitude towards cybersecurity significantly impacted a person's behavioural intention, however subjective norms had an insignificant impact on behavioural intention to use cybersecurity (Aigbefo et al., 2022). Hong & Furnell (2022) found that both attitude towards cybersecurity and perceived behavioural control positively impacted behavioural intention to use cybersecurity, however subjective norms have an insignificant impact (Hong & Furnell, 2022). Both Vrhovec et al. (2023) and Ma (2022) found that perceived behavioural control and subjective norms have a positive impact on the intention to use cybersecurity (Ma, 2022; Vrhovec et al., 2023).

Several academics have confirmed the viability of utilising the TPB to elucidate the process by which cybersecurity behaviours are formed (Dinev & Hu, 2007; Lee & Kozar, 2005). Additionally, numerous studies have noted that intention is

a crucial determining factor in affecting a change in behaviour (Ajzen, 1991; Farooq et al., 2019; Jafarkarimi et al., 2016; Sommestad et al., 2017; Thompson et al., 2017; Whittaker & Noteboom, 2019; Yoon et al., 2012).

As noted by Alanazi et al. (2022) however, this view has also been challenged by various scholars (Hassan et al., 2016; Safa et al., 2015; Shah & Agarwal, 2020; Sheeran & Webb, 2016; Shropshire et al., 2015). To address the disparagement that intention leads to action, Alanazi et al. (2022) added perceived awareness of cyber threats (PACT) as an additional factor to the existing TPB as part of conceptual model and posit that knowledge of cyber threats and skill and knowledge in online information security will have an influence on PACT, which will impact cybersecurity behaviour. The study went on to note certain limitation, one being that other factors related to social, personal and demographic constructs should be examined in future (Alanazi et al., 2022). In Malaysia, a study on enhancing technology adoption in SMEs also suggested that further research needs to be done to identify barriers to the adoption of technology, and the need to evaluate the various technology adoption theories such as the Technology Acceptance Model (Loo et al., 2023).

The theory provides a theoretical foundation for understanding the influence of attitude, perceived behavioural control, and subjective norms on the implementation of cybersecurity among South African SMEs. This will help in exploring the strategies for enforcing cybersecurity policies and understanding the factors that influence cybersecurity compliance and awareness among SMEs in South Africa. This study proposes the inclusion of the perceived ease of use (PEU) and perceived usefulness (PU), which are the two independent variables from the TAM. The conceptual model integrates the elements of the TAM, including PEU and PU. The objective of integrating this theory is to analyse the relationship between the factors (Ali et al., 2022).

2.7.2 Technology Acceptance Model (TAM)

The TAM was originally proposed by Davis (1985), and adapted from the Theory of Reasoned Actions by Ajzen and Fishbein (1980) (Ajzen, 1980; Davis, 1985). As depicted in Figure 2. TAM has four major variables – Perceived Usefulness (PU), Perceived Ease of Use (PEU), Behavioural Intention (BI), and actual Behaviour (B), and suggests that an individual's perception of the usefulness of the technology and the perceived ease of use, results in acceptance of the technology and the intention to make use of it, which results in actual usage of the technology (Lee et al., 2003). TAM is suggested where the specific technology adoption is in its introductory phase (Sánchez-Prieto et al., 2017), hence it being relevant for the adoption of cybersecurity in South Africa.

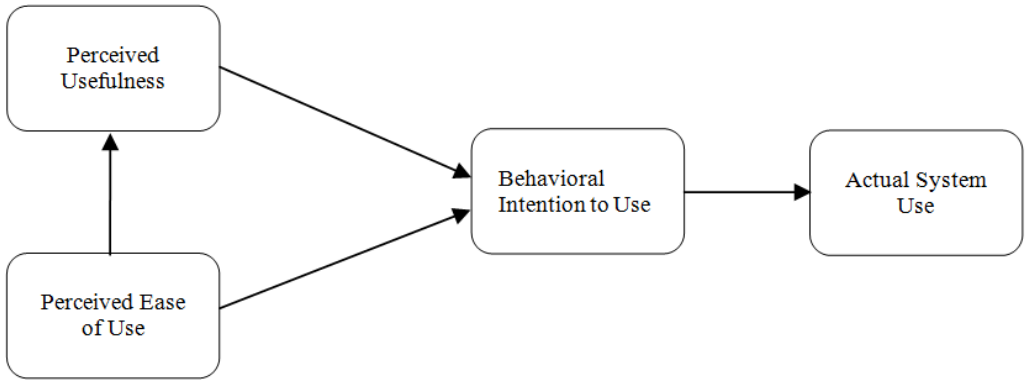


Figure 3: The Technology Acceptance Model

The TAM posits that the behavioural intention to use is a major influencing factor to actual usage of a system (Teo, 2012). Researchers Mun and Hwang (2003), in their quantitative study, found a significant influence between the behavioural intention to use and actual usage (Mun & Hwang, 2003). The perceived ease of use (PEU) of a system is influenced by various aspects, including the user's computer self-efficacy, their perception of control and capacity to learn the system, their level of general computer anxiety, which has a negative connotation, the possible enjoyment they anticipate from using the system, and their intrinsic incentive to utilise it. Perceived usefulness (PU), however, is

influenced by factors such as the actual level of simplicity in using the system, the norms of usage within the business, the overall relevance of the system to the work, and the improved quality of output (Vorm & Combs, 2022).

Perceived ease of use and perceived usefulness both have an influence on the attitude to use a technology, and perceived ease of use has a direct impact on the perceived usefulness, which is essentially a person's perception that using a certain technology will improve their productivity in one way or another (Davis et al., 1989). Perceived ease of use is related to the view that using a specific technology will be relatively easy and free of any major effort from the person and is posited to have a direct impact on the perceived usefulness of a technology. Part of the same study, Davis et al. (1989) suggested that perceived usefulness does not have an impact on perceived ease of use (Davis et al., 1989).

In numerous studies linked to online banking uptake, perceived ease of use is identified as having a positive effect on the users intention (Bashir & Madhavaiah, 2015; Dash et al., 2011; Yoon & Steege, 2013). In a Turkish study on digital banking, Celik (2008) conquered that perceived ease of use plays a significant role in the intention to adopt digital banking (Celik, 2008). Al-Somali et al. (2009) and Amin (2009) both highlighted the positive impact that perceived ease of use has in the online banking space in Saudi Arabia and Malaysia respectively (Al-Somali et al., 2009; Amin, 2009).

Also in the digital banking field of research, studies in Malaysia highlight that perceived usefulness as the most significant variable linked to the adoption of digital banking (Amin, 2009; Tan et al., 2010). Bashir & Madhavaiah (2015) used the TAM model to conduct research on internet adoption within the Indian economy, and also found that perceived usefulness positively impacts the intention to adopt a technology (Bashir & Madhavaiah, 2015). Numerous other studies worldwide, share the same findings that perceived usefulness has a direct and positive impact on the adoption of technology (Al-Somali et al., 2009; Celik, 2008; Jaruwachirathanakul & Fink, 2005; Tan et al., 2010; Yiu et al., 2007; Yoon & Steege, 2013).

2.8 CONCEPTUAL FRAMEWORK

A conceptual framework provides a summarised view, often in graphical form, of the variables of a phenomenon, and indicates their assumed relationships with each other (Miles & Huberman, 1994). The below conceptual framework will be utilised to investigate the level of understanding of cybersecurity, cyber threats and cybersecurity frameworks amongst South African SME owners, and to analyse the factors which affect the implementation of cybersecurity within these SMEs. The Theory of Planned Behaviour (TPD) and the Technology Acceptance Model (TAM), which are behavioural and technology adoption theories respectively, will underpin the quantitative survey.

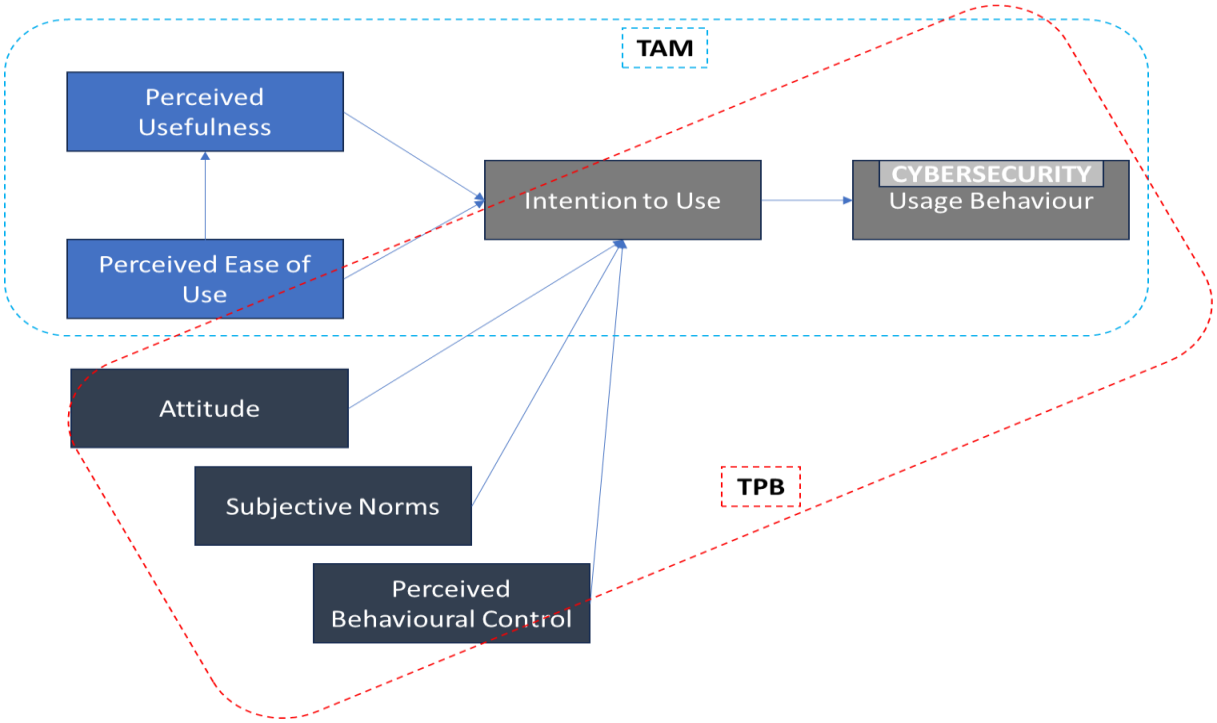


Figure 4: Conceptual Framework

The key elements of the conceptual model will be the independent variables namely, perceived usefulness, perceived ease of use, attitude, subjective norms and perceived behavioural control, and the dependent variables, intention to use and actual usage behaviour. The study will seek to identify the factors that affect the implementation of cybersecurity among SMEs in South Africa, ascertain the

level of agreement that SME owners attach to cybersecurity implementation challenges, determine the relationship between the factors, and determine the influence of selected demographic variables on the identifies factors.

2.9 Conclusion of Literature Review

The literature review contains a comprehensive analysis of cyberspace, cybersecurity, cybersecurity frameworks, the NIST CSF and the King IV report. Based on a review of the literature, it becomes evident that SMEs lack the awareness, knowledge and skills related to cybersecurity and therefore are targets of cybercriminals. Globally, many researchers have looked at how aspects such as awareness, regulation, and resources impact SMEs when it comes to cybersecurity, however in the South African context, there is a lack of research in the cybersecurity space.

The literature review also provides insights into the Theory of Planned Behaviour (TPB) and the Technology Acceptance Model (TAM) and as the two theoretical models and concludes with the conceptual framework.

CHAPTER 3. RESEARCH METHODOLOGY

The purpose of this survey is to investigate the factors that affect cybersecurity implementation, and to create cybersecurity awareness among SMEs in South Africa. This chapter presents the research methodology employed in this study to address the research objectives. The chapter begins with the philosophical orientation that guided the research methodology. The chapter then presents the research design, data collection and analyses methods, and population and sampling methods utilised. The chapter concludes with possible limitations and challenges, quality assurance and ethical considerations that were considered.

3.1 Research approach

This research report followed the quantitative methodology and was guided by the postpositivist worldview. Postpositivists follow a deterministic worldview in which causes lead to effects, and the scientific method is approved. Hence, the research problems examined by postpositivists indicate the need to identify and evaluate the causes that influence outcomes. This philosophy is also reductionist in nature in that ideas are reduced into smaller portions to test, known as variables (Creswell & Creswell, 2018). In this case, cybersecurity implementation is the dependent variable, perceived usefulness, perceived ease of use, attitude, subjective norms, and perceived behavioural control are the independent variables.

Through a postpositivist lens, knowledge is derived from careful observation and measurement of the objective reality. Thus, for a postpositivist, developing numerical measures of observations and analysing the behaviour of individuals is crucial. The belief of postpositivists is that there are theories or laws that govern the world; therefore a researcher should begin with a theory, collect data which will either support or challenge the theory, implement the necessary changes and conduct further tests (Creswell & Creswell, 2018)

3.2 Research design

Research designs are categories of inquiry within the various research methodologies, which specify the procedures in a research study (Creswell & Creswell, 2018). A research design is also referred to as strategy of inquiry (Denzin & Lincoln, 2011). The fundamental purpose of a research design is to ensure that the evidence gathered during a research project enables the researcher to answer the initial research objectives as accurately as possible (De Vaus, 2001).

For this research, a survey design was employed. Survey design allows the ability to conduct a quantitative analysis and description of the trends, attitudes, and sentiments of a population or tests for associations between different variables within a population by probing a sample of that population (Ghauri et al., 2020). A survey design allows the researcher to answer descriptive questions, questions with regards to the relationship between variables, as well as questions about the predictive relationship between variable over a period of time (Creswell & Creswell, 2018). A survey research design was selected to answer the research objectives related to the factors that affect the implementation of cybersecurity among SME owners in South Africa. The design was cross-sectional, as data was collected at a point in time and not over a period of time (Creswell & Creswell, 2018). The survey was emailed to the participants and posted on LinkedIn and WhatsApp to maximise reach.

3.3 Data collection methods

Data collection is a crucial part of the overall research process. It consists of the systematic gathering of information in order to answer the research objectives (Murthy & Bhojanna, 2009). This study made use of both secondary and primary data collection methods. Secondary data sources are easily accessible and were previously collected for other purposes, including academic articles, journals, and reports from industry specialist (Ghauri et al., 2020). Secondary data sources

were deployed to fulfil the theoretical research objectives of the study. The sources for secondary research were academic journals, books, reports from industry experts and web-based sources from credible databases such as Emerald, Sage, Sabinet Online, ScienceDirect, and Google Scholar.

From a primary data collection perspective, this study deployed a survey to collect data to fulfil the research objectives of investigating to investigate the factors that affect cybersecurity implementation, and to create cybersecurity awareness among SMEs in South Africa. This approach was chosen to reach a satisfactory number of respondents. The survey was emailed to respondents and distributed via LinkedIn and WhatsApp.

3.4 Population and sample

The proficient implementation of sampling methods holds considerable importance in augmenting the quality of acquired data. It represents a systematic process that facilitates researchers in accurately characterizing the target population, ascertaining the optimal sample size, and making informed choices regarding the most appropriate sampling technique to employ. (Malhotra & Birks, 2007)

3.4.1 Target population

The target population for a study refers to a collection of objects that can provide the information which the researcher requires, or for who extrapolations could be made (Malhotra & Peterson, 2006). The target population for this study consists of SME owners from all industries within the borders of South Africa.

3.4.2 Sample and sampling method

A sampling method indicates the way the sample will be selected. There are probability sampling methods such as cluster sampling, stratified sampling, systematic sampling, simple-random sampling, and non-probability sampling

methods such as convenience sampling, judgemental/purposive sampling, snowball sampling and quota sampling (Creswell & Creswell, 2018). For this study, convenience sampling was selected. Convenience sampling was chosen due to its ease of implementation, cost-effectiveness and it being an opportune way to collect data.

To derive the sample size for this quantitative study on SMEs, various papers were reviewed to get an understanding of a suitable sample size. A quantitative analysis looking into the factors that impact the adoption of electronic data among Bruneian SMEs had a sample size of 50 SMEs (Seyal et al., 2007). A study that analysed the relationship between entrepreneurial orientation and organisational performance in SMEs employed a sample of 164 SMEs (Kraus et al., 2012). 55 SMEs were surveyed to understand various knotted leadership paradoxes (Henriksen et al., 2021),150 SMEs were the sample size for another study which embarked on understanding whether intellectual capital allows for an improvement in innovation (Agostini et al., 2017), and 81 SMEs were considered sufficient when analysing ERP implementation within SMEs (Deltour, 2012). An average of the above papers was taken; therefore, the target sample size will be 100 SME owners. Aligned to the above method, an online sample size tool called Raosoft was utilised, which returned a sample size of 96 (Raosoft, 2004).

From a response perspective, the demographic findings revealed a diverse participant profile, providing valuable context for interpreting the study results. The age distribution spans various groups, with a notable concentration in the "31 - 40 years" category, signifying a predominantly younger sample. The gender distribution indicated a higher representation of males, albeit with a substantial female presence. One thing to point out was the significant overrepresentation of Indian respondents due to the researcher’s network, while varying representation exists among other racial categories. The industry distribution reflected diversity, particularly in Financial Services, Telecommunications/ICT, Retail, and Healthcare. Therefore overall, the sample aligns well with the broader population

from an Industry and Age perspective but was not representative from a Race perspective.

3.5 The measuring instrument

As noted previously, the research instrument used in this study was a survey. The survey contains questions that will provide the insights required to satisfy the research objectives (Chipeta, 2019). Attention was given to the construction of the survey and its questions, to ensure that it is well designed and conducive for good engagement with the research participants, while also ensuring that the research objectives will be sufficiently answered. To this end, attention was given to the information being requested in the survey, the content and wording of each question, to ensure that they tie back to the research objectives.

The survey has two sections. Section 1 consists of 40 questions and covers the following sub-sections: subjective norms (questions 1 – 4), attitudes (questions 5 – 10), perceived behavioural control (questions 11 – 17) (Rajab & Eydgahi, 2019), perceived ease of use (questions 18 – 23), perceived usefulness (questions 24 – 29) (Davis, 1989), academic/professional background/computer security skills (questions 30 – 40) (Rajivan et al., 2017). Section 2 consists of 10 demographic questions. There are 50 questions altogether, all intended to investigate the factors that affect cybersecurity implementation, and to create cybersecurity awareness among SMEs in South Africa.

The measures utilised in the survey were reused from previous research by Rajab & Eydgahi (2019) who investigated the role that theoretical frameworks play when it pertains to the intention to conform with information security procedures, Davis (1989) who looked at factors that impact a user's acceptance of information technology, and Rajivan et al. (2017) who explored the factors required to measure user acceptance of information security. Questions which were not relevant for the purpose of the study were removed to ensure the data collected

is relevant and will assist to fulfil the research objectives (Davis, 1989; Rajab & Eydgahi, 2019; Rajivan et al., 2017).

The measurement instruments used in these studies have often undergone testing for validity and reliability, therefore making use of these scales can ensure that the intended constructs accurately and consistently measured. Acknowledging and utilising the work of previous researchers by using their validated scales is a form of intellectual honesty and respect for the research community. It also helps to avoid potential bias that could arise from developing and using untested or less reliable measurement tools. The Cronbach alfa/factor analysis scores were all over 0.7 indicating that the measure scale accurately measures the intended constructs. One of the contributing factors of reusing existing measurements scales was due to the time constraints of the study. For this reason, a pilot test was not conducted.

3.6 Procedure for data collection

The target population was contacted via LinkedIn, WhatsApp, and email. All SMEs were provided with context before participating in the survey. Each participant was provided with the purpose of the research, how the data will be utilised, and confidentiality was assured. The digital nature of the survey allowed the participants to complete the survey seamlessly without printing and scanning documents and enabled easy collation of the data.

Social media and email were selected due to the convenience factor, considering the time limitations to complete the research. Social media provides the ability to reach a large and diverse audience quickly and efficiently. The survey approach also enhances data collection efficiency, reduces logistical challenges, keeps costs low, and ensures timely responses.

To understand the credibility of the study, it is important to consider the representativeness of the sample obtained through social media platforms like LinkedIn and WhatsApp, and email. While these channels offer a convenient way

to reach a large audience, they may introduce certain biases that could affect the generalisability of the findings. The sample may over-represent individuals and SMEs that are digitally literate and have easy access to online platforms. This could exclude a portion of the population, particularly those in rural areas or less tech-savvy sectors, leading to a skewed understanding of the broader SME landscape. LinkedIn tends to cater to professionals and businesses that are more established or actively engaged in networking. This could result in an over-representation of more formal, perhaps better-resourced SMEs, while under-representing smaller, less connected businesses. Participants via WhatsApp would be due to the researcher's convenience, and may have similar interests, so self-selection bias may come into play. These respondents may have a particular interest in cybersecurity or may already be aware of its importance, potentially skewing the results towards a more informed or concerned demographic. These biases may diminish the generalisability of the survey. Data collection began in October and continued throughout November and December; therefore, the process took 3 months. The survey was started by 157 SME owners. Of the 157, 79 surveys were partially completed so they were not included in the analysis. Therefor the analyses is based on 78 completed surveys Data cleaning and analysis began in December once a satisfactory number of responses were received. This included checking for incomplete surveys, coding, and results. January was spent finalising the analysis, report writing, and submission to my supervisor for review and updates. This was repeated until the finished product was submitted on the 29th of February 2024

3.7 Data analysis strategies and interpretation

Data analysis is the transformation of unprocessed data into information that can be used to draw conclusions about a phenomenon (Ghauri et al., 2020). This study deployed descriptive statistics, factor analysis, correlation analysis, Cronbach alpha analysis and Analysis of Variance (ANOVA) test. Descriptive statistics provides the capability to summarise and organise the data in a meaningful way (Lomax & Hahs-Vaughn, 2013). Descriptive data analysis was

used to organise the demographic data. Descriptive statistics were used to summarise and organise the data, providing a clear overview of the sample's characteristics, and offering insights into the general trends and distributions within the sample. It provided the foundational understanding and was the initial step for more complex analysis. The purpose of employing factor analysis to a study is to simplify the interpretation and comprehension of relationships and patterns (Yong & Pearce, 2013). Factor analysis was utilised to analyse the factors that impede the implementation of cybersecurity, and to compare and validate the results with what the literature and theoretical models propose. This assisted in assessing whether the identified factors align with existing literature, enhancing the study's theoretical grounding. Correlation analysis is flexible data analysis method that can be applied when a quantitative variable must be examined as a function of or in relation to any other factors of interest (Cohen et al., 1983). In this case, correlation analysis was used for multicollinearity, to ensure that the independent variables used in further analyses, do not distort the results by being too similar. Cronbach’s alpha analysis is a measure of the intercorrelations between different indicators that capture certain constructs (Ghauri et al., 2020), and was used to determine reliability of measuring instrument. Reliability is crucial for ensuring that the measurement instruments used consistently reflect the construct being measured. ANOVA is a statistical tool that can be used to obtain more precise data based on the maximum, minimum, and mean average (Hassan et al., 2024). The one-way ANOVA test was run to determine the influence of the selected demographic variables on the identified factors. By doing so, it can be determined if different demographic groups perceive or are affected by cybersecurity issues differently, which can inform targeted interventions or policies. Due to the number of respondents, it is important to note the possible limitations such as reduced generalisability, potential instability in factor analysis, and challenges in detecting multicollinearity.

3.8 Possible limitations and challenges of the study

The primary objective of this study is to investigate the cybersecurity implementation challenges among South African SMEs, with a focus on investigating the influence that perceived ease of use, perceived usefulness, attitude, perceived behavioural control, and subjective norms has on the implementation of cybersecurity among SMEs in South Africa. The target population for this study consists of SME owners from all industries within the borders of South Africa that were reachable via LinkedIn, WhatsApp and email. Therefore, the findings of the study are limited to the context and cannot be generalised to the wider population. In addition, time limitations to reach the proposed sample size were posed a challenge, and there were numerous surveys that could not be utilised due to incomplete questions, and respondents starting but not completing the survey.

3.9 Quality Assurance

3.9.1 External validity OR transferability

Validity refers to the degree to which a collection of measured things accurately represents the underlying theoretical concept that the items are intended to measure (Clark & Watson, 2019). Gathering information from the SME owners directly increases the external validity.

3.9.2 Internal validity OR credibility

Internal validity refers to the extent to which a research study can demonstrate that the observed effects or outcomes are due to the independent variables being studied, rather than other factors (FitzPatrick, 2019). Internal validity and credibility were met by making use of tried and tested theories such as the Technology Acceptance model (TAM) and the Theory of Planned behaviour (TPB) as the underpinning of the conceptual model. Cybersecurity definitions,

literature and models were obtained from credible databases and industry experts.

3.9.3 Reliability OR dependability

Reliability in a research paper refers to the consistency and stability of the measurement instruments or procedures used in the study (Sürücü & Maslakci, 2020). Reliability in this study was met by careful consideration when compiling the survey to ensure that the data collected and captured, meets the requirements of the research objectives.

3.10 Ethical considerations

This research was classified as low risk as the study does not include any vulnerable categories, does not involve any question that may invoke harm or uneasiness on the participants. The participants were provided with clear context, advised about the purpose of the study and how their information will be used.

All information shared will remain confidential and only used for the purposes of the study. No information was shared with other participants and business names are not mentioned in the final research project. All owner and business information will remain anonymous as far as can be controlled.

3.11 Proposed schedule and timelines

Figure 5 below indicates the project plan for this research project. The month of July entailed defending the research proposal. The panel feedback indicated that the proposal required enhancement. The feedback was incorporated, and an updated proposal was submitted in August, and on the 28th of August, ethical clearance was received. Once approvals were received, the questionnaire was reviewed, and amendments were made before kicking off data collection. Data collection began in October and continued throughout November and December.

Data cleaning and analysis began in December once a satisfactory number of responses were received. This included checking for incomplete surveys, coding, and results. January was spent finalising the analysis, report writing, and submission to my supervisor for review and updates. This was repeated until the finished product was submitted on the 29th of February 2024. Underpinning this plan was continuous engagement and alignment with my supervisor to iteratively improve the research report.

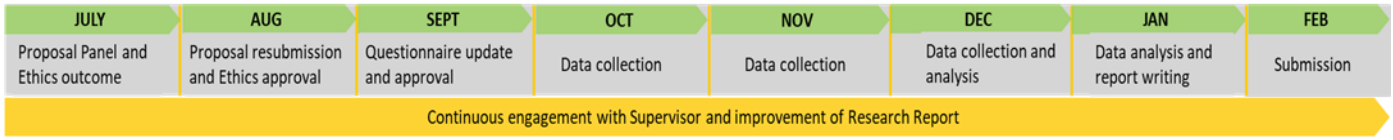


Figure 5: Research report project plan

CHAPTER 4. PRESENTATION AND INTERPRETATION OF RESULTS

This chapter focuses on the presenting and discussing the results of the survey. The primary objective of this study is to investigate the cybersecurity implementation challenges among South African SMEs, by investigating the influence that perceived ease of use, perceived usefulness, attitude, perceived behavioural control, and subjective norms have on the implementation of cybersecurity among SMEs. IBM Statistical Package for Social Sciences (SPSS version 28) was utilised for data analysis.

4.1 Introduction

The main purpose of the survey is to identify the factors that affect the implementation of cybersecurity among SMEs in South Africa, ascertain the level of agreement that SME owners attach to cybersecurity implementation challenges, determine the relationship between the factors, and determine the influence of selected demographic variables on the identifies factors.

The survey was started by 157 SME owners. Of the 157, 79 surveys were partially completed so they were not included in the analysis. Therefore, the following analyses is based on 78 completed surveys. The subsequent sections provide insights into the empirical findings.

4.2 Results pertaining to Research Objective

4.2.1 Reliability Analysis

Reliability is the degree to which a measuring tool consistently represents the variable it is measuring (Field, 2013). Cronbach's alpha analysis is a measure of the intercorrelations between different indicators that capture certain constructs (Ghauri et al., 2020), and was used to determine reliability of measuring

instrument. Malhotra (2020) asserts that Cronbach's alpha values below 0.6 suggest inadequate internal consistency, whereas values above 0.6 suggest adequate internal consistency (Malhotra, 2020). The following sections unpacks the reliability across the various subsections in the survey.

Subjective norms:

Reliability Statistics	
Cronbach's Alpha	N of Items
.914	4

Table 4.1: Subjective norms reliability analysis

The Cronbach's alpha coefficient of 0.914 indicates a very high level of internal consistency for the 4 question items related to the variable subjective norms. This suggests that the items are reliably measuring the variable of subjective norms among the respondents.

Attitude:

Reliability Statistics	
Cronbach's Alpha	N of Items
.871	6

Table 4.2: Attitude reliability analysis

The Cronbach's alpha coefficient of 0.871 suggests a high level of internal consistency for the 6 question items related to attitude. This indicates that the items are reliably measuring the variable of attitude among the respondents.

Perceived Behavioural Control:

Reliability Statistics	
Cronbach's Alpha	N of Items
.871	7

Table 4.3: Perceive behavioural control reliability analysis

The Cronbach's alpha coefficient of 0.871 indicates a high level of internal consistency for the7 question items related to the variable perceived behaviour control. This suggests that the 7 items are reliably measuring the variable of perceived behaviour control among the respondents.

Perceived Ease of Use:

Reliability Statistics	
Cronbach's Alpha	N of Items
.932	6

Table 4.4: Perceived ease of use reliability analysis

The Cronbach's alpha coefficient of 0.932 indicates a very high level of internal consistency for the 6 question items related to perceived ease of use. This suggests that the 6 items are reliably measuring the variable of perceived ease of use among the respondents.

Perceived Usefulness:

Reliability Statistics	
Cronbach's Alpha	N of Items
.943	6

Table 4.5: Perceived usefulness reliability analysis

The Cronbach's alpha coefficient of 0.943 indicates an extremely high level of internal consistency for the 6 question items related to perceived usefulness. This suggests that the items are reliably measuring the variable of perceived usefulness among the respondents.

The Cronbach alpha scores above indicate good internal consistency across the survey.

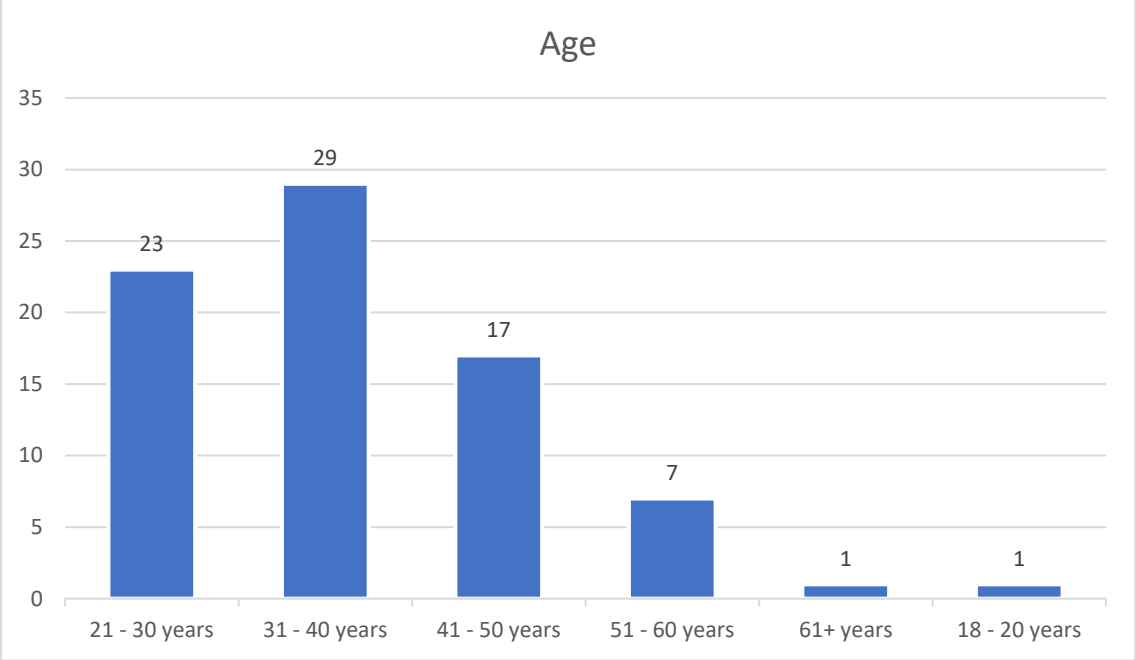
4.2.2 Descriptive Analysis

The below sections describe the make-up for the SME owners who completed the survey and provide a graphical representation of their demographic profile.

Age

The age distribution of the respondents is diverse, with participants spanning across different age groups. The largest age group is "31 - 40 years", constituting 37.2% of the total respondents. This suggests that a significant portion of the sample falls within the age range of 31 to 40 years. The cumulative percent shows that approximately 89.7% of respondents are aged 50 or below. This indicates that many participants are relatively younger. The age group "61+ years" has the lowest representation, with only 1.3% of respondents falling into this category. This might imply a potential limitation in terms of insights from older participants. The diverse age distribution could impact the generalisability of findings. Different age groups may have distinct perspectives, experiences, and attitudes, especially in a study related to cybersecurity where awareness and technology adoption may vary across generations.

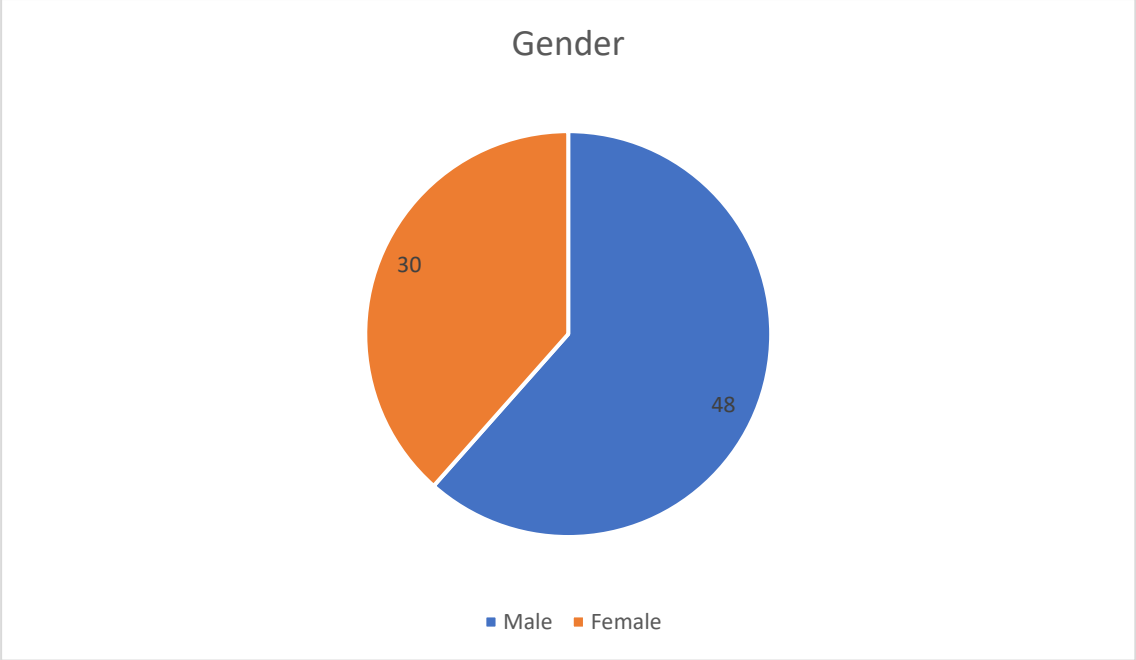
Figure 6: Age descriptive analysis



Gender

The gender distribution of the respondents indicates a mix of male and female participants. Many of the respondents identify as male, constituting 61.5% of the total sample. This suggests a higher representation of males in the study. The female respondents make up 38.5% of the total sample. While this percentage is lower than that of males, it still represents a sizable portion of the participants.

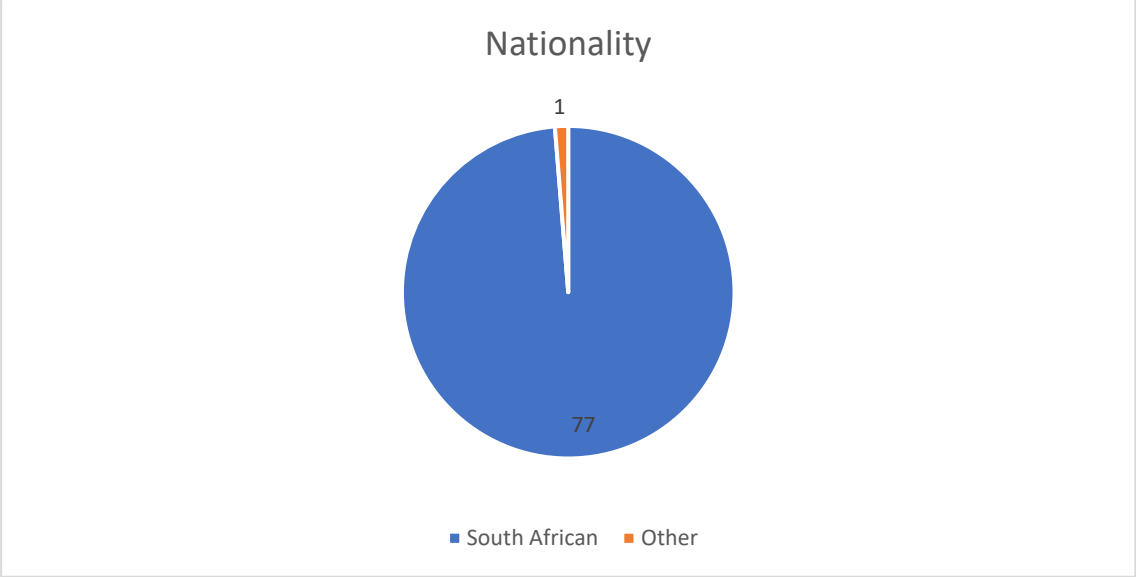
Figure 7: Gender descriptive analysis



Nationality

The nationality distribution of the respondents indicates a predominant representation of South African participants. The vast majority (98.7%) of the respondents identify as South African. This suggests that the study primarily includes participants from South Africa. Only a small percentage (1.3%) of respondents indicated a nationality other than South African. While this group is a minority in the sample, acknowledging their representation is important for considering diversity. The high representation of South African participants suggests that the findings may be more applicable to the South African context, which aligns to the purpose of the study.

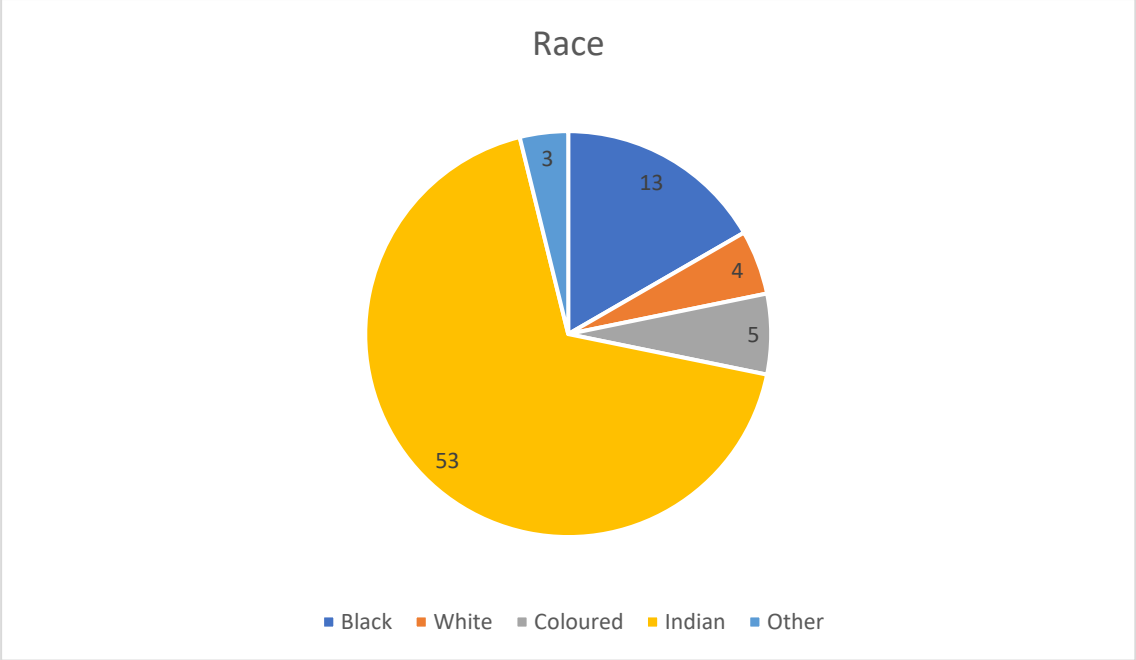
Figure 8: Nationality descriptive analysis



Race

The frequency distribution reflects a diverse sample with representation from multiple racial categories. Many respondents (67.9%) identify as Indian. White respondents have the lowest representation, comprising only 5.1% of the total sample. This may impact the ability to draw robust conclusions about the experiences and perspectives of this racial group. Black, Coloured, and Other racial categories make up the remaining portion of the sample. While smaller in number, these groups contribute to the overall racial diversity of the respondents. The cumulative percent column shows the proportion of the sample accounted for by each racial category. The top three categories (Indian, Black, and Coloured) make up the majority of respondents.

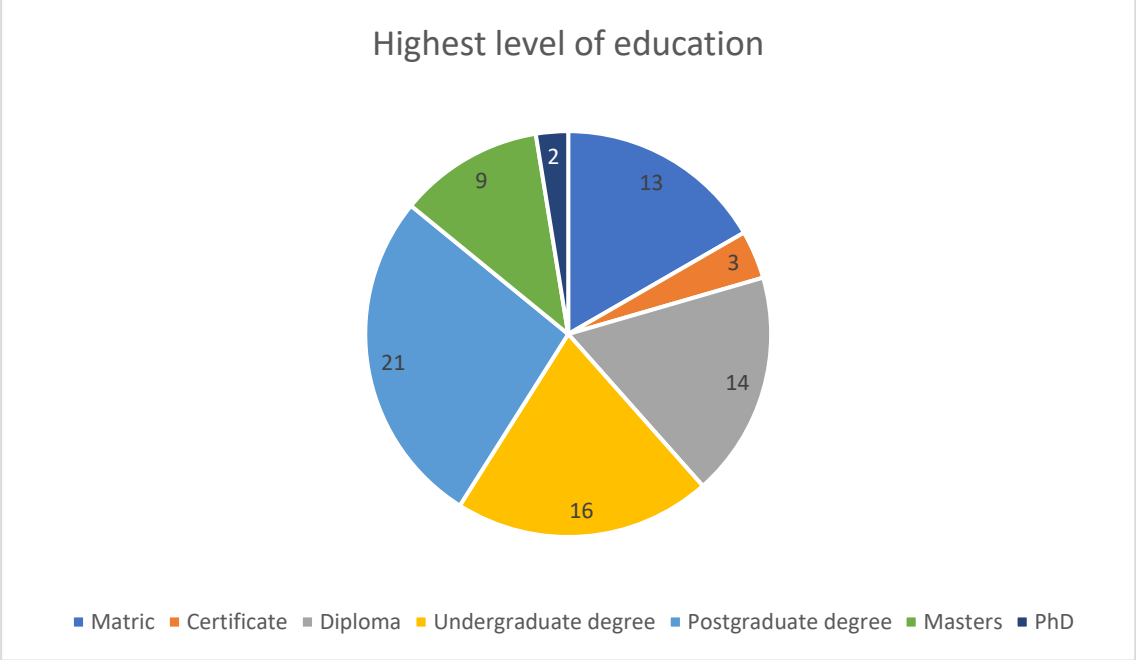
Figure 9: Race descriptive analysis



Highest level of education

The frequency distribution illustrates a diverse range of education levels among the respondents. Postgraduate degrees (including master's and PhD) are well represented, constituting a significant portion of the sample (26.9% to 38.5%). This suggests a higher proportion of respondents with advanced education. Undergraduate degrees are also present, with 20.5% of respondents holding an undergraduate degree. This group contributes to the diversity of educational backgrounds. Matric (secondary education) and certificate holders are present but form a smaller percentage of the sample. This diversity in education levels allows for insights across a spectrum of academic qualifications. The cumulative percent column shows the proportion of the sample accounted for by each education level. The top three categories (Postgraduate, Undergraduate, and Diploma) make up the majority of respondents.

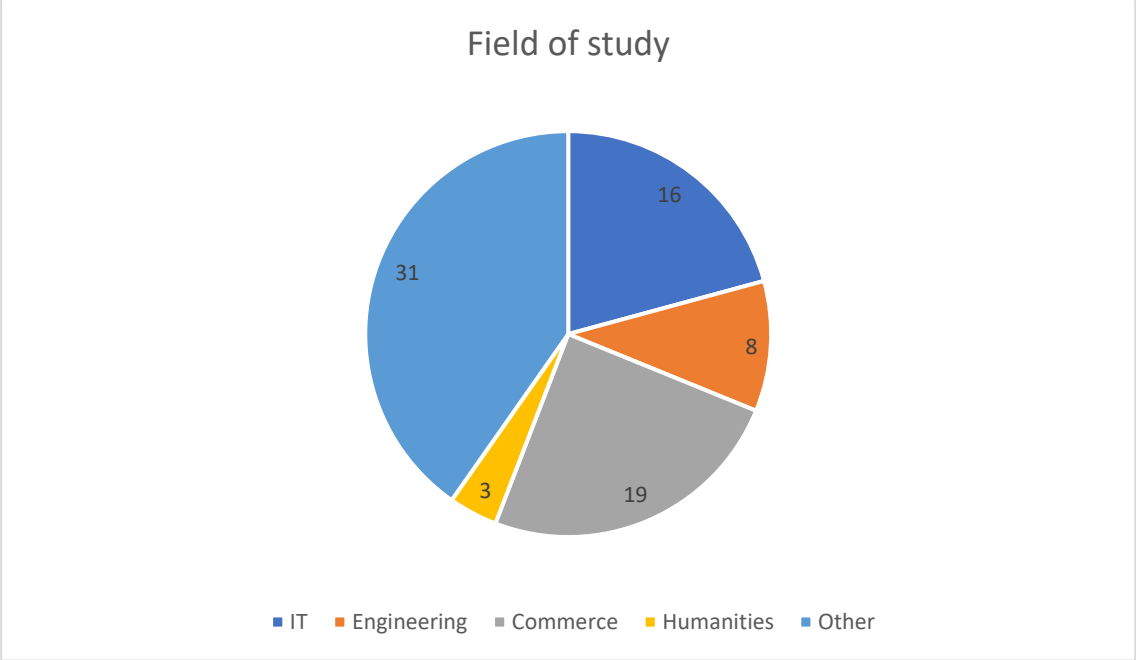
Figure 10: Education descriptive analysis



Field of study

The frequency distribution reveals diversity in the fields of study among the respondents. IT and Commerce are the most common fields of study, with 20.8% and 24.7% of respondents, respectively. This suggests a significant representation of individuals with backgrounds in these fields. Engineering is the third most common field of study, with 10.4% of respondents. While not as prevalent as IT and Commerce, it still contributes to the diversity of academic backgrounds. Humanities, represented by 3.9% of respondents, and Other fields, comprising 40.3%, contribute to the overall diversity. The "Other" category includes a range of diverse fields not explicitly listed. The top three categories (IT, Commerce, and Engineering) make up many respondents. Different fields of study may influence how individuals perceive and approach cybersecurity.

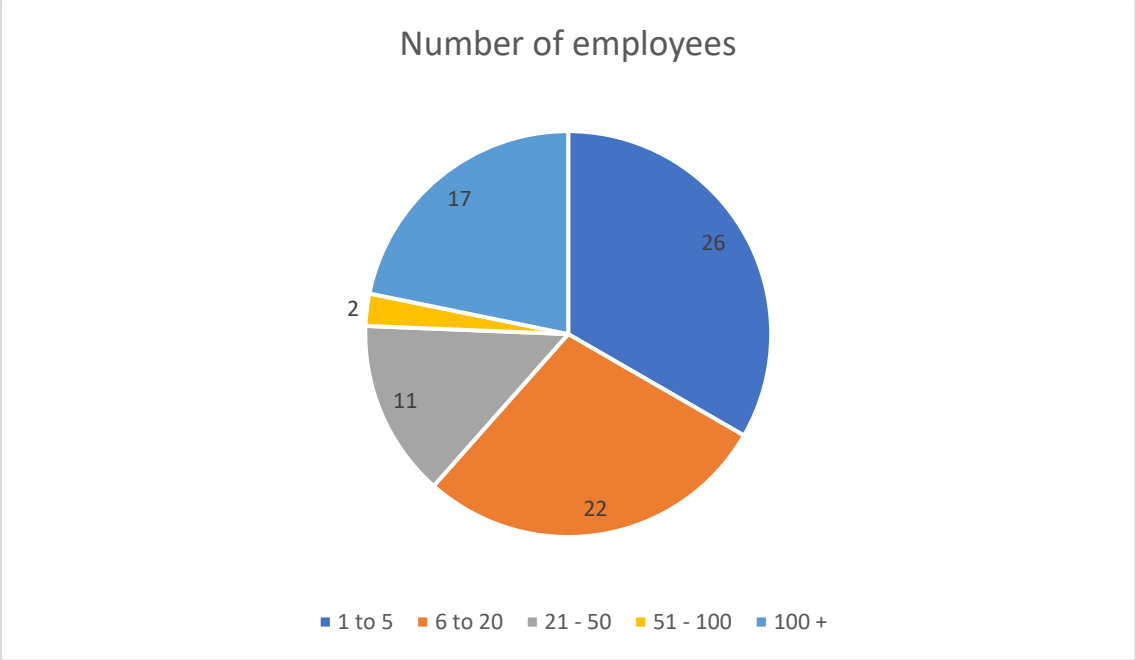
Figure 11: Field of study descriptive analysis



Number of employees

The frequency distribution reveals a variety in the reported number of employees across different SME categories. Many respondents own smaller businesses, with 33.3% reporting 1 to 5 employees and 28.2% reporting 6 to 20 employees. SMEs with 21 to 50 employees and 51 to 100 employees have a smaller representation, accounting for 14.1% and 2.6%, respectively. SMEs with one hundred or more employees make up a substantial portion of the sample, comprising 21.8%. This indicates a significant presence of larger SMEs in this study. The top two categories (1 - 5 and 6 - 20 employees) make up the majority of respondents. Due to its size, this type of SME can influence its cybersecurity practices and challenges. Smaller organisations may face resource and skill constraints, and security needs compared to larger SMEs.

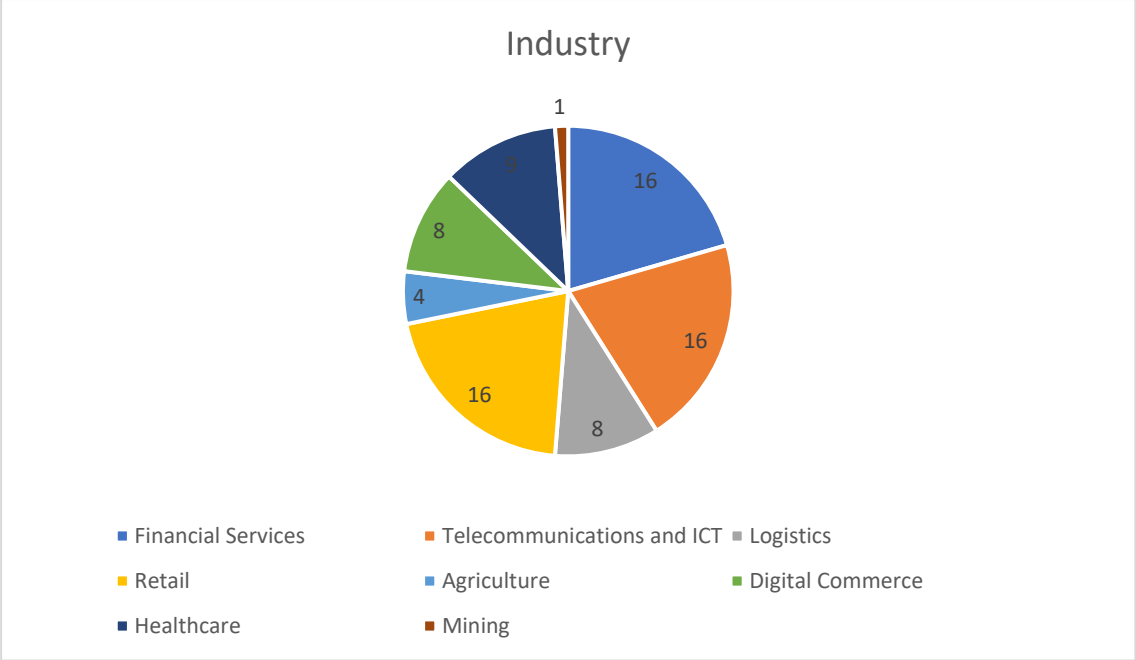
Figure 12: Number of employees descriptive analysis



Industry

The frequency distribution reflects diversity in the industries represented by the respondents. Financial Services and Telecommunications and ICT are the most prevalent industries, each accounting for 20.5% of respondents. This indicates a significant representation from these sectors. Retail and Healthcare also have substantial representation, with 20.5% and 11.5% of respondents, respectively. These industries contribute to the overall diversity in the sample. Digital Commerce has a notable presence, constituting 10.3% of the sample. Given the increasing role of digital platforms, this representation is relevant to discussions on cybersecurity in the digital realm. The top four industries (Financial Services, Telecommunications/ICT, Retail, and Healthcare) make up the majority of respondents.

Figure 13: Industry descriptive analysis



In conclusion, the demographic findings revealed a diverse participant profile, providing valuable context for interpreting the study results. The age distribution spans various groups, with a notable concentration in the "31 - 40 years" category, signifying a predominantly younger sample. The gender distribution indicated a higher representation of males, albeit with a substantial female presence. South African participants overwhelmingly dominated the nationality category, highlighting the study's focus on a specific geographical context. The racial distribution showcased significant overrepresentation of Indian respondents, while varying representation exists among other racial categories. Education levels were diverse, with a notable presence of postgraduate degree holders, reflecting a sample with advanced educational backgrounds. Fields of study encompass a range of disciplines, with IT and Commerce prevailing. Organisational sizes varied, emphasising the inclusion of both smaller enterprises and larger corporations. The industry distribution reflected diversity, particularly in Financial Services, Telecommunications/ICT, Retail, and Healthcare.

4.2.3 Correlation Analysis

The correlation analysis results provide valuable insights into the relationships between the factors of the study and answer the third empirical objective of the study ("To determine the relationship between the factors"). Correlation analysis is flexible data analysis method that is applied when a quantitative variable must be examined in relation to any other factors of interest (Cohen et al., 1983). In this case, correlation analysis was used for multicollinearity. The study utilised the Pearson correlation coefficient (r) to analyse the degree to which the factors, subjective norms, attitude, perceived behavioural control, perceived ease of use, and perceived usefulness, are associated. The results are discussed in the following sections.

Correlations

		Subjective Norms	Attitude	Perceived Behavioural Control	Perceived Ease of Use	Perceived Usefulness
Subjective Norms	Pearson Correlation	1	,554**	,214	,140	,437**
	Sig. (2-tailed)		<,001	,060	,222	<,001
Attitude	Pearson Correlation	,554**	1	,506**	,271*	,653**
	Sig. (2-tailed)	<,001		<,001	,016	<,001
Perceived Behavioural Control	Pearson Correlation	,214	,506**	1	,655**	,569**
	Sig. (2-tailed)	,060	<,001		<,001	<,001
Perceived Ease of Use	Pearson Correlation	,140	,271*	,655**	1	,551**
	Sig. (2-tailed)	,222	,016	<,001		<,001
Perceived Usefulness	Pearson Correlation	,437**	,653**	,569**	,551**	1
	Sig. (2-tailed)	<,001	<,001	<,001	<,001	

Table 4.6: Correlation analysis

Subjective norms and Attitude:

There is a moderate to strong positive correlation ($r = 0.554$, $p < 0.01$) between subjective norms and attitude. The positive correlation suggests that respondents who perceive strong norms favouring information security policy adherence are more likely to have positive attitudes towards cybersecurity implementation. This indicates that subjective norms play a role in shaping attitudes.

Attitude and Perceived behavioural control:

There is a strong positive correlation ($r = 0.506$, $p < 0.01$) between attitude and perceived behavioural control. The positive correlation implies that individuals with positive attitudes towards cybersecurity are likely to perceive higher control over their ability to implement cybersecurity measures, emphasising the interplay between attitudes and perceived control.

Perceived behavioural control and Perceived Ease of Use:

There is a strong positive correlation ($r = 0.655$, $p < 0.01$) between perceived behavioural control and perceived ease of use. The moderate to strong positive correlation indicates that individuals who feel in control of cybersecurity measures are more likely to perceive these measures as easy to use. This suggests that a sense of control contributes to the perceived ease of implementing cybersecurity, supporting the study's empirical objectives.

Perceived Ease of Use and Perceived Usefulness:

There is a strong positive correlation ($r = 0.551$, $p < 0.01$) between perceived ease of use and perceived usefulness. The positive correlation suggests that individuals who find cybersecurity measures easy to use are more likely to perceive them as useful, indicating that perceived ease of use contributes to the perceived utility of cybersecurity measures.

Subjective norms and Perceived Usefulness:

There is a significant positive correlation ($r = 0.437$, $p < 0.01$) between subjective norms and perceived usefulness. The positive correlation implies that respondents who perceive strong norms in favour of cybersecurity are more likely to find cybersecurity tools and frameworks useful.

In summary, the correlation analysis revealed strong relationships between the factors, emphasising the interconnected nature of factors influencing cybersecurity implementation among South African SMEs. The lowest correlation worth highlighting is subjective norms and perceived ease of use ($r = 0.140$, $p < 0.01$) and attitude and perceived ease of use ($r = 0.271$, $p = 0.016$). This indicates that respondents who think that they should be using, and have positive attitudes towards cybersecurity tools, believe that making use of cybersecurity in practice is not easy. Overall, the results were significant, which aligns with what the literature states, and highlights that attitude (Al-Debei et al., 2013; Cheung & To, 2016; Law, 2020; Mohit et al., 2023; Song et al., 2018; Sun et al., 2017), subjective norms (Dholakia & Soltysinski, 2001; Lee & Geistfeld, 1998; Li, 2007; Nafees et al., 2021; Rahman et al., 2020; Rau et al., 2008; Todd & Benbasat, 2000), and perceived behavioural control (Bautista et al., 2022; Cheung & To, 2016; Chu et al., 2016), perceived ease of use (Bashir & Madhavaiah, 2015; Dash et al., 2011; Yoon & Steege, 2013), and perceived usefulness (Al-Somali et al., 2009; Celik, 2008; Jaruwachirathanakul & Fink, 2005; Tan et al., 2010; Yiu et al., 2007; Yoon & Steege, 2013) are crucial factors in shaping cybersecurity practices.

4.2.4 Factor Analysis

Factor analysis was utilised to answer the first and second empirical objectives (“To identify the factors that affect the implementation of cybersecurity among SMEs in South Africa”; and “To ascertain the level of agreement that SME owners attach to cybersecurity implementation challenges”) of the study. The purpose of employing factor analysis to a study is to simplify the interpretation and

comprehension of relationships and patterns (Yong & Pearce, 2013). Exploratory factor analysis seeks to analyse the relationship between variables without specifically assessing how well this relationship conforms to a predefined model (Chipeta, 2019). The specific test utilised on IBM-SPSS (version 28) was the Kaiser-Meyer-Olkin (KMO). The following sections delve into the results.

Subjective Norms

Subjective norms was measured using 4 items. Item 1 had an eigenvalue of 3.192 and 79.81% of the variance, indicating that item 1 contributes significantly to the subjective norm factor. Item 2 explains 10.08% of the total variability in the dataset, as represented by its eigenvalue of 0.403. Item 3 and 4 have eigenvalues of 0.295 and 0.110, and they explain 7.37% and 2.74% of the total variance respectively.

Total Variance

	Initial Eigenvalues			Extraction Sums of Squared Loadings		
Item	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	3.192	79.806	79.806	3.192	79.806	79.806
2	.403	10.080	89.886			
3	.295	7.370	97.256			
4	.110	2.744	100.000			

Table 4.7: Subjective norms total variance

The extraction column indicates the proportion of variance that is accounted for by the identified questions under subjective norms. All scores were above 0.5. Item 1, “My business partners think that I should follow the information security policy” was the highest with 0.865, which indicate that the variable is well represented by the identified factors. The statement highlights the importance and relevance of the specific item in capturing perceptions about following

information security policies, based on its strong association with the factors identified in the analysis.

Communalities	
	Extraction
1. My business partners think that I should follow the information security policy	.865
2. My colleagues think that I should follow the information security policy	.859
3. Our IT department pressures me to follow its information security policy	.691
4. My subordinates think that I should follow the information security policy	.778

Table 4.8: Subjective norms communalities

Overall, there is good communality. The identified factors explain a substantial proportion of the variance in each variable, with the first two items being particularly well captured. The items, particularly item 1, captured a significant portion of the variability in respondents' perceptions of subjective norms regarding information security policies.

These findings suggest that subjective norms related to cybersecurity implementation are well captured by the identified items, with a dominant role played by the perceptions of business partners and colleagues.

Attitude

Attitude was measured using 6 items. Item 1 had an eigenvalue of 3.836 and 63.94% of the variance, indicating that item 1 contributes considerably to the attitude factor. Items 2 and 3 explain 14.89% and 10.83% of the total variability in the dataset, as represented by its eigenvalues of 0.894 and 0.650 respectively. Item 6 has an eigenvalue of 0.153, and it explains 2.54% of the total variance.

Total Variance						
	Initial Eigenvalues			Extraction Sums of Squared Loadings		
Item	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	3.836	63.937	63.937	3.836	63.937	63.937
2	.894	14.892	78.829			
3	.650	10.833	89.661			
4	.261	4.345	94.007			
5	.207	3.449	97.456			
6	.153	2.544	100.000			

Table 4.9: Attitude total variance

The extraction column indicates the proportion of variance that is accounted for by the identified questions under attitude. Notably all scores were above 0.5, besides Item 6. Item 4, “Following our information security policy is a necessary” was the highest with 0.776, which indicate that the variable is well represented by the identified factors. Item 6, “Following our information security policy is pleasant”, was lowest with 0.294, which indicates that this variable has a lower communality, suggesting it might be less well represented by the identified factors. Overall, findings of the above table highlights that the identified items explain a substantial proportion of the variance in each variable, with some variability in how well each variable is captured expect for item 6, as it recorded a low communality value of 0.294.

Communalities	
	Extraction

1. The preventative measures available to me to stop people from gaining access to business information are adequate	.647
2. The preventative measures available to prevent people from causing damage to our information systems are adequate	.598
3. Following our information security policy is a good idea	.770
4. Following our information security policy is a necessary	.776
5. Following our information security policy is beneficial	.751
6. Following our information security policy is pleasant	.294

Table 4.10: Attitude communalities

Attitudes related to the perceived adequacy of preventative measures and the positive perception of following information security policies are well captured by the identified factors. These findings suggest that attitudes related to the perceived adequacy of preventative measures and positive perceptions of following information security policies are well captured by the identified questions.

Perceived Behavioural Control

Perceived behavioural control was measured using 7 items. Item 1 had an eigenvalue of 4.264 and 60.92% of the variance, indicating that item 1 contributes strongly to the perceived behavioural control factor. Items 2 and 3 explain 14.00% and 7.27% of the total variability in the dataset, as represented by its eigenvalues of 0.980 and 0.509 respectively. Item 7 has an eigenvalue of 0.170, and it explains 2.43% of the total variance. These findings suggest that the questions

related to the variable perceived behavioural control over cybersecurity measures are well captured by the identified factors.

Total Variance						
	Initial Eigenvalues			Extraction Sums of Squared Loadings		
Item	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	4.264	60.920	60.920	4.264	60.920	60.920
2	.980	14.006	74.926			
3	.509	7.271	82.197			
4	.484	6.916	89.113			
5	.383	5.467	94.580			
6	.210	2.993	97.573			
7	.170	2.427	100.000			

Table 4.11: Perceived behavioural control total variance

The extraction column indicates the proportion of variance that is accounted for by the identified questions under attitude. Notably all scores were above 0.5, besides Item 5. Item 7, “My ability to prevent cybersecurity breaches at my business is adequate” was the highest with 0.826, which indicate that the variable is well represented by the identified factors. Item 5, “Following our information security policy is pleasant”, was lowest with 0.091, which indicates that this variable has a lower communality, suggesting it might be less well represented by the identified factors. Overall, the identified factors explain a substantial proportion of the variance in each variable, with variability in how well each variable is captured. Item 5, “I can enable cybersecurity measures on my company computer but only when I have manuals for reference” has the lowest communality, suggesting that it might not be well captured by the identified factors.

Communalities	
	Extraction
1. I have the necessary skills to protect my business from cybersecurity violations	.766
2. I have the expertise to implement preventative measures to stop people from accessing confidential business information	.706
3. have the skills to implement preventative measures to stop people from damaging my work computer	.621
4. I believe that 1is w1hin my control to protect myself from cybersecurity violations	.619
5. I can enable cybersecurity measures on my company computer but only when I have manuals for reference	.091
6. For me, taking cybersecurity precautions is easy	.636
7. My ability to prevent cybersecurity breaches at my business is adequate	.826

Table 4.12: Perceived behavioural control communalities

Perceived Ease of Use

Perceived ease of use was measured using 6 items. Item 1 had an eigenvalue of 4.488 and 74.79% of the variance, indicating that item 1 contributes significantly to the perceived ease of use factor. Items 2 and 3 explain 10.75% and 5.26% of the total variability in the dataset, as represented by its eigenvalues of 0.645 and 0.337 respectively. Item 6 has an eigenvalue of 0.052, and it explains 0.87% of the total variance. These findings suggest that the items related to the variable perceived ease of use, as it pertains to cybersecurity, are well captured by the identified factors.

Total Variance		
Item	Initial Eigenvalues	Extraction Sums of Squared Loadings

	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	4.488	74.793	74.793	4.488	74.793	74.793
2	.645	10.748	85.541			
3	.337	5.618	91.159			
4	.273	4.545	95.704			
5	.206	3.429	99.133			
6	.052	.867	100.000			

Table 4.13: Perceived ease of use total variance

The extraction column indicates the proportion of variance that is accounted for by the identified questions under attitude. Notably all scores were above 0.5. Item 6, “I would find cybersecurity concepts, techniques, and frameworks easy to use” was the highest with 0.791, which indicate that the variable is well represented by the identified factors. Overall, the identified factors explain a substantial proportion of the variance in each variable, with some variability in how well each variable is captured.

Communalities	
	Extraction
1. Learning to operate cybersecurity tools and frameworks would be easy for me	.760
2. I would find it easy to get cybersecurity frameworks to work for my business	.780
3. My interaction with cybersecurity concepts and frameworks was clear and understandable	.713
4. I would find cybersecurity concepts and frameworks flexible to interact with	.713
5. I would be easy for me to become skilled in cybersecurity	.731

6. I would find cybersecurity concepts, techniques, and frameworks easy to use	.791

Table 4.14: Perceived ease of use communalities

Perceived Usefulness

Perceived usefulness was measured using 6 items. Item 1 had an eigenvalue of 4.627 and 77.87% of the variance, indicating that item 1 contributes significantly to the perceived usefulness factor. Items 2 and 3 explain 8.21% and 6.12% of the total variability in the dataset, as represented by its eigenvalues of 0.492 and 0.367 respectively. Item 6 has an eigenvalue of 0.096, and it explains 1.60% of the total variance. These findings suggest that the items related to the variable perceived usefulness of cybersecurity tools and frameworks are well captured by the identified factors.

Total Variance Explained

	Initial Eigenvalues			Extraction Sums of Squared Loadings		
Item	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	4.672	77.874	77.874	4.672	77.874	77.874
2	.492	8.207	86.082			
3	.367	6.115	92.197			
4	.252	4.196	96.392			
5	.120	2.008	98.401			
6	.096	1.599	100.000			

Table 4.15: Perceived usefulness total variance

The extraction column indicates the proportion of variance that is accounted for by the identified questions under attitude. Notably all scores were above 0.5. Item 5, “Using cybersecurity tools and frameworks would make it easier to do my job”

was the highest with 0.867, which indicate that the variable is well represented by the identified factors. Overall, the identified factors explain a substantial proportion of the variance in each variable, with some variability in how well each variable is captured.

Communalities	
	Extraction
1. Using cybersecurity tools and frameworks in my business would enable me to accomplish my business goals more quickly	.728
2. Using cybersecurity tools and frameworks would improve my businesses performance	.791
3. Using cybersecurity tools and frameworks in my job would increase my productivity	.856
4. Using cybersecurity tools and frameworks would enhance my effectiveness on the job	.786
5. Using cybersecurity tools and frameworks would make it easier to do my job	.867
6. I would find cybersecurity tools and frameworks useful in my business	.645

Table 4.16: Perceived usefulness communalities

In conclusion, the factor analysis results support the empirical research objectives by revealing the underlying relationships and shared variance among the variables related to subjective norms, attitude, perceived behavioural control, perceived ease of use, and perceived usefulness. The positive correlations and high communalities indicate that these variables are interconnected and contribute significantly to understanding the cybersecurity implementation challenges among South African SMEs. The identified factors provide a foundation for addressing the empirical research objectives by emphasising the importance of subjective norms, attitudes, perceived behavioural control,

perceived ease of use, and perceived usefulness in the context of cybersecurity implementation.

4.2.5 ANOVA Test

ANOVA is a statistical tool that can be used to obtain more precise data based on the maximum, minimum, and mean average (Hassan et al., 2024). The one-way ANOVA test was run to test the fourth empirical objective ("To determine the influence of the selected demographic variables on the identified factors") of the study. Below are the results of the ANOVA analysis to determine the influence that age has on subjective norms, attitude, perceived behavioural control, perceived ease of use, and perceived usefulness.

Age

ANOVA			
		F	Sig.
Subjective Norms	Between Groups	2.196	.064
Attitude	Between Groups	.613	.690
Perceived Behavioral Control	Between Groups	.229	.948
Perceived Ease of Use	Between Groups	.988	.431
Perceived Usefulness	Between Groups	.238	.945

Table 4.17: ANOVA using age

Subjective norms:

- F-statistic: 2.196
- p-value: 0.064 (slightly greater than 0.05)

The p-value is close to the significance level of 0.05, suggesting a marginally significant difference in subjective norms among different age groups.

Attitude:

- F-statistic: 0.613
- p-value: 0.690 (greater than 0.05)

The one-way ANOVA results indicate no statistically significant difference in attitude among different age groups. The p-value is well above 0.05.

Perceived behavioural control:

- F-statistic: 0.229
- p-value: 0.948 (greater than 0.05)

There is no statistically significant difference in perceived behavioural control among different age groups. The p-value exceeds 0.05.

Perceived Ease of Use:

- F-statistic: 0.988
- p-value: 0.431 (greater than 0.05)

The one-way ANOVA results suggest no statistically significant difference in perceived ease of use among different age groups. The p-value is above 0.05.

Perceived Usefulness:

- F-statistic: 0.238
- p-value: 0.945 (greater than 0.05)

There is no statistically significant difference in perceived usefulness among different age groups. The p-value is above 0.05.

Overall conclusion**,** there is no significant difference in attitude, perceived behavioural control, perceived ease of use, and perceived usefulness among the different age groups. However, there is a marginally significant difference in subjective norms among different age groups.

ANOVA tests were also run across the multifaceted demographic variables of age, gender, race, number of employees, industry, highest level of education, field of study, and nationality, the comprehensive analyses indicated a noteworthy coherence in employees' perspectives on cybersecurity-related factors. Remarkably, these demographic factors do not appear to exert substantial influence on subjective norms, attitudes, perceived behavioural control, perceived ease of use or perceived usefulness. This uniformity underscores the universality of employees' perceptions concerning cybersecurity measures, advocating for the development of universally applicable cybersecurity awareness programs and tools. While recognising this general consistency, organisations may benefit from targeted efforts to address specific nuances within industries, such as the marginally significant variations in computer security skills. This nuanced approach aligns with the overarching conclusion that a comprehensive, yet tailored, cybersecurity strategy is essential for fostering a robust and inclusive cybersecurity culture within diverse organisational contexts.

4.3 Discussion of results

The comprehensive analysis of various aspects related to cybersecurity implementation among South African SMEs provided valuable insights into the factors influencing this critical domain. The study explored respondents' perceptions regarding subjective norms, attitudes, perceived behaviour control, perceived ease of use, and perceived usefulness. Notably, there was a consensus among respondents in favour of following information security policies, as evidenced by low mean values and a predominant selection of "Strongly Agree."

The study also revealed a positive attitude toward the adequacy of preventative measures, albeit with some variability. Respondents generally expressed moderate levels of perceived behavioural control, perceived ease of use, and perceived usefulness regarding cybersecurity measures and tools. Additionally, academic, and professional backgrounds aligned positively with computer security skills for most participants.

The correlation analysis unveiled significant relationships between variables, suggesting interconnectedness in respondents' perceptions. Notably, attitudes and perceived usefulness exhibited strong positive correlations, emphasising the interconnected nature of these variables. Factor analysis further supported the validity of the selected variables, with high extraction communalities indicating that the identified factors effectively explain the observed variances. The demographic analysis shed light on the diverse characteristics of the respondent sample, including age, gender, nationality, race, education, field of study, number of employees, and industry representation.

Considering the research objectives, the findings contributed to identifying factors affecting cybersecurity implementation among South African SMEs, laying the groundwork for understanding perceptions and challenges in this context. The study also offered a basis for creating cybersecurity awareness by uncovering prevalent attitudes and perceptions among SMEs. The demographic information provided a nuanced understanding of the diverse sample, acknowledging potential variations in perspectives based on demographics.

In summary, the results align with the literature in that attitude (Al-Debei et al., 2013; Cheung & To, 2016; Law, 2020; Mohit et al., 2023; Song et al., 2018; Sun et al., 2017), subjective norms (Dholakia & Soltysinski, 2001; Lee & Geistfeld, 1998; Li, 2007; Nafees et al., 2021; Rahman et al., 2020; Rau et al., 2008; Todd & Benbasat, 2000), and perceived behavioural control (Bautista et al., 2022; Cheung & To, 2016; Chu et al., 2016), perceived ease of use (Bashir & Madhavaiah, 2015; Dash et al., 2011; Yoon & Steege, 2013), and perceived usefulness (Al-Somali et al., 2009; Celik, 2008; Jaruwachirathanakul & Fink,

2005; Tan et al., 2010; Yiu et al., 2007; Yoon & Steege, 2013) all play fundamental roles in impacting the intention to behave in a certain way, which then leads to actual change in behaviour.

Looking at the variables from the TPD first, Aigbefo et al. (2022) opined that attitude towards cybersecurity significantly impacted a person's behavioural intention, however subjective norms had an insignificant impact on behavioural intention to use cybersecurity (Aigbefo et al., 2022), however the results are not aligned with this view. The correlation analysis indicates moderate to strong correlation between these factors, suggesting interconnectedness in respondents' perceptions of these two factors. The factor analysis results confirmed this. Similarly, Hong & Furnell (2022) found that both attitude towards cybersecurity and perceived behavioural control positively impacted behavioural intention to use cybersecurity, however subjective norms have an insignificant impact (Hong & Furnell, 2022). Again, the results indicate that subjective norms, attitude and perceived behavioural control are all crucial factors for determining the intention to use cybersecurity tools.

From a TAM perspective, numerous studies linked to online banking uptake, perceived ease of use is identified as having a positive effect on the users intention (Bashir & Madhavaiah, 2015; Dash et al., 2011; Yoon & Steege, 2013). Similarly, a number of studies worldwide, share the same findings that perceived usefulness has a direct and positive impact on the adoption of technology (Al-Somali et al., 2009; Celik, 2008; Jaruwachirathanakul & Fink, 2005; Tan et al., 2010; Yiu et al., 2007; Yoon & Steege, 2013). This research aligns with these previous paper as noted by the results of the study.

Interesting result to note is between subjective norms, perceived ease of use and attitude. The lowest correlation worth highlighting is subjective norms and perceived ease of use ($r = 0.140$, $p < 0.01$) and attitude and perceived ease of use ($r = 0.271$, $p = 0.016$), which indicates that respondents who think that they should be using, and have positive attitudes towards cybersecurity tools, believe that making use of cybersecurity in practice is not easy. Therefore, there would

be benefit in creating cybersecurity content, and a basic, practical framework for SMEs to use.

Not part of the core factors of the study, Academic Professional Background and Computer Security Skills was also measure. Looking into the results, the findings indicate that a majority of respondents perceive a positive alignment between their academic or professional background and computer security skills. The highest frequency is observed in the category with a value of 1.82, indicating that a significant number of respondents fall into this category. By the 1.82 category, approximately 79.5% of respondents fall into this category or a lower one. This suggests that a substantial majority of respondents have relatively high mean values in the 1.00 to 1.82 range. It is evident that higher values represent a more positive perception of the alignment between academic or professional background and computer security skills. The findings indicate that a majority of respondents perceive a positive alignment between their academic or professional background and computer security skills, emphasising the importance of education and training when it comes to cybersecurity.

The analysis provided a robust foundation for addressing the main objective of the study. The insights gained from the statistical analyses and interpretations contributed to a deeper understanding of the challenges and factors influencing cybersecurity implementation among South African SMEs, paving the way for targeted interventions and policy recommendations. This research laid the groundwork for a comprehensive exploration of cybersecurity issues within the context of SMEs, offering valuable implications for practitioners, policymakers, and researchers in the field. With 78 completed surveys, this should be noted as a limitation.

CHAPTER 5. CONCLUSIONS & RECOMMENDATIONS

5.1 Introduction

The new digital era has led to new opportunities for businesses to reach wider audiences, improve operational efficiencies, and create new revenue streams. Digitalisation also poses challenges for businesses, with cybercrime being a significant problem for modern businesses (Mphatheni & Maluleke, 2022). While large enterprises have more resources to invest in cybersecurity, smaller businesses often encounter resource constraints due to the absence of an earmarked cybersecurity budget and requisite expertise, thereby impeding their ability to keep up the pace with evolving technologies and security threats (Gafni & Pavel, 2019). As many SMEs move towards improved ways of doing business, utilising the cloud and internet services, their cyber risk is increasing (Hemant et al., 2011). Pawar & Palivela (2022) suggests that SMEs have a higher average cost per employee related to data breaches as compared to large enterprises (Pawar & Palivela, 2022).

To this end, the primary objective of this study was to investigate the cybersecurity implementation challenges among South African SMEs. The study was underpinned by the Theory of Planned Behaviour and the Technology Acceptance Model, which formed the contextual framework. The aim was to identify the factors that affect the implementation of cybersecurity among SMEs in South Africa, ascertain the level of agreement that SME owners attach to cybersecurity implementation challenges, determine the relationship between the factors, and determine the influence of selected demographic variables on the identifies factors.

The following sections will highlight key takeouts related to the objectives of the study, followed by recommendations to create cybersecurity awareness amongst SMEs.

5.2 Conclusions regarding the research objectives

The primary objective of this study is to investigate the cybersecurity implementation challenges among South African SMEs. As such, the study explored respondents' perceptions regarding subjective norms, attitudes, perceived behaviour control, perceived ease of use, and perceived usefulness, and aimed to answer the below sub-objectives. The comprehensive analysis of various aspects related to cybersecurity implementation among South African SMEs provided valuable insights into the factors influencing cybersecurity implementation.

- To identify the factors that affect the implementation of cybersecurity among SMEs in South Africa

The factor analysis results support the research objective by revealing the underlying relationships and shared variance among the variables related to subjective norms, attitude, perceived behaviour control, perceived ease of use, and perceived usefulness. The analysis and high communalities indicate that these variables are contribute significantly to understanding of the cybersecurity implementation challenges faced by South African SMEs. The identified factors provide a foundation for addressing the research objectives by emphasising the importance of subjective norms, attitudes, control perceptions, ease of use, and usefulness perceptions in the context of cybersecurity implementation.

- To ascertain the level of agreement that SME owners attach to cybersecurity implementation challenges

The analysis suggests that there is a high level of agreement among SME owners that the identified factors (subjective norms, attitude, perceived behaviour control,

perceived ease of use, and perceived usefulness) are closely related and contribute significantly to the understanding of cybersecurity implementation challenges.

- To determine the relationship between the factors

The strong positive correlations among subjective norms, attitude, perceived behaviour control, perceived ease of use, and perceived usefulness indicated interconnectedness. Notably, there is a significant positive correlation ($r = 0.437$, $p < 0.01$) between subjective norms and perceived usefulness. The positive correlation implies that respondents who perceive subjective norms in favour of cybersecurity are more likely to find cybersecurity tools and frameworks useful.

Overall, these factors collectively contribute to explaining the influences of cybersecurity implementation. The findings emphasised the need to consider these factors holistically, as they may influence each other and collectively impact the implementation of cybersecurity practices.

- To determine the influence of selected demographic variables on the identified factors

Across the multifaceted demographic variables of age, gender, race, number of employees, industry, highest level of education, field of study, and nationality, the comprehensive analyses indicated a noteworthy coherence in SME owners' perspectives on cybersecurity-related factors. Remarkably, these demographic factors do not appear to exert substantial influence on subjective norms, attitudes, perceived behavioural control, perceived ease of use or perceived usefulness. This uniformity underscores the universality of SME owners' perceptions concerning cybersecurity measures, advocating for the development of broadly applicable awareness and training initiatives. While recognising this general consistency, organisations may benefit from targeted efforts to address specific nuances within industries, such as the marginally significant variations in computer security skills. This nuanced approach aligns with the overarching conclusion that a comprehensive, yet tailored, cybersecurity strategy is essential

for fostering a robust and inclusive cybersecurity culture within diverse organisational contexts.

5.2.1 Implications considering the technological, economic and social issues

The global technology landscape is constantly evolving, which results in new cybersecurity threats and vulnerabilities emerging regularly. As SMEs in South Africa and globally adopt technologies like cloud computing, AI, and IoT, the complexity of their cybersecurity needs increase, highlighting the need for SMEs to integrate cybersecurity tools into their technology adoption strategies. The focus on perceived ease of use and perceived usefulness of cybersecurity tools among SMEs can be tied to the importance of these tools being adaptable and user-friendly, to keep pace with these changes.

From an economic perspective, cybersecurity threats can have significant financial consequences for SMEs, potentially leading to business disruptions or closure, financial losses, and loss of customer trust. The ability of SMEs to compete in both local and global markets increasingly depends on their cybersecurity posture. The economic pressures on SMEs, particularly in developing economies like South Africa, make it crucial to implement cost-effective cybersecurity solutions which are scalable, and can be widely adopted by SMEs.

From a social perspective, individuals, communities, businesses irrespective of their size, governments and regulatory institutions need to understand the concept of cybersecurity, its importance and the consequences if not adopted. This involves education and awareness initiatives that align with global best practices, not only technical solutions. An important consideration is the global shortage of skilled cybersecurity professionals. This will have an implication on society as a whole, and SMEs, who may struggle to find and afford qualified personnel.

5.3 Recommendations

Based on the findings, which confirmed that perceived ease of use, perceived usefulness, attitude, perceived behavioural control, and subjective norms indeed influence the implementation of cybersecurity, the below are recommendations to improve the cybersecurity posture within SMEs in South Africa.

5.3.1 Enhance perceived ease of use through training and user-friendly tools

To foster a strong cybersecurity culture, SMEs should invest in regular training programs that educate employees about the latest threats, phishing scams, data protection practices, and the proper use of cybersecurity tools. Such programs should be tailored to the specific needs of SMEs, focusing on practical, actionable advice that employees can implement immediately. These initiatives should align with global best practices, ensuring that SMEs are not only compliant with local regulations but also equipped to handle threats that transcend national borders.

Customised cybersecurity training programs designed for SMEs can greatly improve their awareness, understanding, and compliance with security policies (Bada & Nurse, 2019). There are numerous cybersecurity specialist companies in South Africa, such as Cybersecurity Institute, who provide cybersecurity training to employees, management and leadership (https://cybersecurityinstitute.co.za/academy/, 2024). There are many other global options, as well as training providing by consulting firms in South Africa. In addition, offering SMEs cybersecurity tools and technologies, which are easy to use, can help employees comply with security policies and procedures, and make it easy for employees to implement cybersecurity practices (Kim et al., 2020). As mentioned previously, the NIST is a common cybersecurity framework that can provide a set standards that are implemented by specialised tools designed to capture and analyse enterprise-level information security auditing (National Institute of Standards and Technology, 2017). If a formal cybersecurity framework

is not relevant, there are numerous tools available from cybersecurity specialists that will assist SMEs with understanding their basic security needs, multi-factor authentication, cloud security, endpoint security detection, and incident response (Aung, 2023).

This could be practically implemented as follows:

Step 1 – Assess Training Needs: Conduct a needs assessment by surveying SMEs to identify current knowledge gaps and understand the specific cybersecurity challenges they face. This will enable clear understanding of the training needs for different roles within the SME, ensuring that the program is relevant and targeted. Based on the assessment, identify essential topics such as phishing awareness, data protection, password management, secure use of devices, and compliance with local regulations.

Step 2 – Develop a customised training program: Decide on the format that best suits SMEs, whether it be in-person workshops, online courses, webinars, or a blended approach. Partner with training providers who specialise in SME needs, to develop high-quality, relevant content.

Step 3 – Implement the training program: Engage the SME community to agree on how best to do this. Set up a training calendar that includes regular sessions across industries and types of SMEs. Deliver the training using interactive methods such as simulations, role-playing, and quizzes to keep SMEs engaged and ensure they understand how to apply what they've learned. Supplement training with easily accessible resources like cheat sheets, video tutorials, and FAQs that SMEs can refer to as needed.

Step 4 – Monitor and evaluate training: After each training session, conduct post-session feedback to understand what worked well, and what could be enhanced. Collate the feedback and ensure iterative improvement of the training.

Step 5 – Ensure ongoing training and updates: Plan for periodic refresher courses to update SMEs on new threats, evolving best practices, and any changes in

regulations. Promote a culture where cybersecurity awareness is part of the daily routine, encouraging SMEs to stay informed and share knowledge. A similar step-by-step plan can be implemented to create awareness, to foster a positive cybersecurity culture, to setup a resources and support model, and to ensure peer and industry engagement happens.

5.3.2 Emphasize perceived usefulness through awareness and with demonstrated benefits

Cybersecurity awareness is a foundational element in building a resilient defence against cyber threats. For SMEs in South Africa, where resources may be limited, cultivating a culture of cybersecurity awareness is crucial. This involves embedding cybersecurity principles into the day-to-day operations of the business and ensuring that all employees, regardless of their role, understand the importance of protecting the organisation from cyber threats. Emphasizing the perceived usefulness of cybersecurity measures involves creating awareness, and effectively communicating the tangible benefits that implementing such measures can bring to South African SMEs. SME owners need to highlight the benefits of cybersecurity measures in terms of protecting sensitive data, preventing financial losses, and safeguarding business reputation (Davis et al., 1989). Benefits such as 1) the protection of sensitive information, which includes customer information, intellectual property, and financial records (Herath & Rao, 2009); 2) the prevention of financial losses, which could possibly include expenses to restore systems, cost of investigating a breach, the cost of recovering lost data, and possible legal and regulatory fees (Cavusoglu et al., 2004); and enhancing the business' reputation by publicly advocating cybersecurity best practice and adhering to industry standards, which will foster integrity, reliability and hold the SME in high stead with customers, partners, suppliers, and government alike (Kim & Mueller, 1978).

5.3.3 Foster positive attitudes towards cybersecurity through leadership, clear communication, and culture

The role of leadership in promoting a cybersecurity culture cannot be overstated. SME owners and managers must lead by example, demonstrating a commitment to cybersecurity that permeates the entire business. This can be achieved by encouraging open discussions about cybersecurity challenges and leading by example. The is a need to promote a cybersecurity-positive culture within SMEs through leadership endorsement, clear communication of cybersecurity policies, and recognition of employees' efforts in adhering to security practices (Straub et al., 2004). Leaders who demonstrate commitment to cybersecurity by setting a positive example, allocating resources, and actively supporting security initiatives can positively influence employee attitudes and behaviours (Gale et al., 2022). Clear communication of cybersecurity policies, accompanied by the justification for their implementation, will enhance an employee's understanding of cybersecurity requirements and fosters a culture of compliance (Vance et al., 2012). Additionally, acknowledging, and incentivising employees for their adherence to security measures encourages desirable behaviours and fosters the promotion of a security-aware culture. This could involve recognising employees who report security incidents, engage in training programs, or exhibit exceptional compliance with cybersecurity standards (Gallaugher, 2011).

5.3.4 Facilitate perceived behavioural control with resources and support

Provide SMEs with resources such as cybersecurity experts, budget allocations, and technical support to facilitate the implementation of security measures (Ajzen, 1991). Without sufficient budget allocations for cybersecurity, business may face difficulty in implementing robust solutions related to investing in technology, training programs, and security measures that are necessary to safeguard against ever-changing cyber threats (Whitman & Mattord, 2021). The provision of technical support and access to cybersecurity experts, including is crucial in addressing security concerns, and improves an employees' perceived

ability to control their behaviour by providing support and guidance in implementing security measures (D'Arcy & Hovav, 2007).

5.3.5 Leverage subjective norms through peer influence and industry standards

Encourage SMEs to participate in industry forums, collaborate with peers, and adhere to cybersecurity standards and regulations to align with prevailing norms (Lu et al., 2017). Collaboration with peers and participation with industry forums, enables interpersonal exchanges, which have a substantial impact on employees' attitudes and behaviours towards security measures. SMEs can utilise these engagements to encourage compliance with cybersecurity standards and norms (Siponen et al., 2014). Furthermore, adherence to cybersecurity standards acts as a framework for desirable security behaviours and assists in establishing norms within a business. SMEs should conform to industry standards in order to showcase their commitment to cybersecurity and promote a security-aware culture (Egelman & Peer, 2015).

5.3.6 Encourage cybersecurity partnerships across all stakeholders

To make a real impact, cybersecurity efforts need to be owned and championed by numerous stakeholders, not only individuals, businesses and government. There is a need to collaborate with educational institutions such as schools, universities, and technical colleges to develop specialised cybersecurity courses and certification programs tailored for SMEs. These programs could focus on practical skills that employees and business owners need to protect their enterprises from cyber threats. As part of this initiative, establish internship and apprenticeship opportunities for students in cybersecurity programs, allowing them to work directly with SMEs. This would not only provide SMEs with affordable access to cybersecurity expertise but also give students real-world experience. At a school level, basic information security should become part of the computer studies curriculum.

In addition, non-governmental organisations, as the liaison between the government and the public, must be engaged to support with creating awareness and assisting with advocating for the relevant policies. NGOs involved in cybersecurity can play a crucial role in raising awareness among SMEs by conducting workshops, webinars, and community outreach programs. These initiatives can be tailored to the specific needs and challenges faced by SMEs in different regions of South Africa. NGOs can also advocate for policies that support SME cybersecurity, such as government subsidies for cybersecurity training or tax incentives for investing in cybersecurity tools. There is also a need to encourage partnerships between SMEs, government agencies, large corporations, and cybersecurity firms to share resources, knowledge, and best practices. Public-private partnerships can help SMEs access advanced cybersecurity tools and expertise that might otherwise be unaffordable. Practically, a partnership where large tech companies provide SMEs with discounted cybersecurity software and training, or a government program that offers free cybersecurity audits for SMEs, would greatly improve the cybersecurity posture within South Africa. This would work particularly well if cybersecurity was incorporated into the broader Corporate Social Responsibility (CSR) initiative in South Africa.

These recommendations aim to address the identified factors influencing cybersecurity implementation among South African SMEs. By implementing these suggestions, SMEs can better protect their digital assets and mitigate cyber risks effectively.

5.4 Limitations

Due to time and financial constraints, the study was limited to the SME owners in the network of the researcher, therefore predominantly SME owners from Gauteng. The sample size was consistent to previous studies conducted on

SMEs, however generalisation to the SME population across South Africa must be carefully considered.

5.5 Suggestions for further research

Further research would enable scholars to contribute to advancing knowledge and understanding of cybersecurity implementation among South African SMEs, thereby informing evidence-based policy interventions and capacity building initiatives to strengthen the resilience of businesses and individuals as it pertains to cybersecurity.

Firstly, future research could employ qualitative or mixed-method research on this topic, which would complement the quantitative findings with in-depth analyses to gain a deeper understanding of the socio-cultural, organisational, and contextual factors that shape SMEs' attitudes and behaviours towards cybersecurity. Qualitative methods such as interviews, focus groups, and case studies can provide nuanced insights into the underlying motivations, perceptions, and decision-making processes related to cybersecurity implementation among SMEs. This would allow for a more comprehensive analysis by validating quantitative findings with qualitative insights.

Secondly, further research on intervention studies to evaluate the effectiveness of targeted cybersecurity awareness campaigns, training programs, and policy interventions aimed at enhancing SMEs' cybersecurity posture is necessary. By measuring the impact of specific interventions on SMEs' cybersecurity practices, researchers can identify best practices and tailor interventions to address the unique needs and challenges faced by different types of SMEs.

Thirdly, due to the lack of cybersecurity literature, there is a need to study cybersecurity implementation challenges over an extended period. A longitudinal study to track the cybersecurity implementation progress and challenges among South African SMEs over an extended period. This approach would provide insights into the sustainability of cybersecurity measures and the evolving nature

of cyber threats faced by SMEs, enabling researchers to identify long-term trends and patterns.

Additionally, future research could be done within specific contexts for example within specific industries or geographical contexts. Future studies on specific industries to explore how specific characteristics influence cybersecurity implementation. This would help in understanding industry-specific challenges and developing tailored solutions. Exploring regional differences within South Africa could reveal how local socio-cultural factors impact SMEs' cybersecurity practices. This is particularly relevant in a country with diverse cultural and economic contexts.

REFERENCES

Agostini, L., Nosella, A., & Filippini, R. (2017). Does intellectual capital allow improving innovation performance? A quantitative analysis in the SME context. *Journal of Intellectual Capital*, *18*(2), 400-418.

Aigbefo, Q. A., Blount, Y., & Marrone, M. (2022). The influence of hardiness and habit on security behaviour intention. *Behaviour & Information Technology*, *41*(6), 1151-1170.

Ajzen, I. (1980). Understanding attitudes and predictiing social behavior. *Englewood cliffs*.

Ajzen, I. (1985). The theory of planned behavior: some unresolved issues. *Organizational Behavior and Human Decision Processes. Special Issue on Theories of Cognitive Self-Regulation*.

Ajzen, I. (1991). The theory of planned behavior. *Organizational behavior and human decision processes*, *50*(2), 179-211.

Al-Debei, M. M., Al-Lozi, E., & Papazafeiropoulou, A. (2013). Why people keep coming back to Facebook: Explaining and predicting continuance participation from an extended theory of planned behaviour perspective. *Decision support systems*, *55*(1), 43-54.

Al-Enezi, K. A., Al-Shaikhli, I. F., Al-Kandari, A. R., & Al-Tayyar, L. Z. (2014). A survey of intrusion detection system using case study Kuwait Governments entities. 2014 3rd International Conference on Advanced Computer Science Applications and Technologies,

Al-Somali, S. A., Gholami, R., & Clegg, B. (2009). An investigation into the acceptance of online banking in Saudi Arabia. *Technovation*, *29*(2), 130-141.

Alanazi, M., Freeman, M., & Tootell, H. (2022). Exploring the factors that influence the cybersecurity behaviors of young adults. *Computers in human behavior*, *136*, 107376.

Alawida, M., Omolara, A. E., Abiodun, O. I., & Al-Rajab, M. (2022). A deeper look into cybersecurity issues in the wake of Covid-19: A survey. *Journal of King Saud University-Computer and Information Sciences*, *34*(10), 8176-8206.

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*, *21*(20), 6901.

Ali, A. B. A., Ayyasamy, R. K., Akbar, R., Ap Ponnusamy, V., & Heng, L. E. (2022). Cybersecurity infrastructure adoption model for malware mitigation in small medium enterprises (SME). 2022 IEEE 5th International Symposium in Robotics and Manufacturing Automation (ROMA),

Ali, N. M., & Wanasilpb, W. (2022). Small and Medium Enterprises (SMEs) Financing Through One Semi-Formal Sector Bank and Five Formal Sector Banks to Create Entrepreneurs: An Empirical Study. *INTERNATIONAL JOURNAL OF TRADE & COMMERCE-IIARTC*.

Alsharida, R. A., Al-rimy, B. A. S., Al-Emran, M., & Zainal, A. (2023). A systematic review of multi perspectives on human cybersecurity behavior. *Technology in Society*, 102258.

Amin, H. (2009). An analysis of online banking usage intentions: an extension of the technology acceptance model. *International Journal of Business and Society*, *10*(1), 27.

Antunes, M., Maximiano, M., & Gomes, R. (2022). A Client-Centered Information Security and Cybersecurity Auditing Framework. *Applied Sciences*, *12*, 1-15. https://doi.org/https://doi.org/10.3390/app12094102

Aung, B. (2023). *SIMPLE CYBER SECURITY MEASURES FOR SMBS TO ENSURE A SAFER DIGITAL LANDSCAPE*. https://www.smetechguru.co.za/simple-cyber-security-measures-for-smbs-to-ensure-a-safer-digital-landscape/

Azmi, R., Tibben, W., & Win, K. T. (2018). Review of cybersecurity frameworks: context and shared concepts. *Journal of cyber policy*, *3*(2), 258-283.

Bada, M., & Nurse, J., R.C. (2019). Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs). *Information & Computer Security*, *27*(3), 393-410. https://doi.org/10.1108/ICS-07-2018-0080

Baker, J. (2012). The technology–organization–environment framework. *Information Systems Theory: Explaining and Predicting Our Digital Society, Vol. 1*, 231-245.

Bashir, I., & Madhavaiah, C. (2015). Consumer attitude and behavioural intention towards Internet banking adoption in India. *Journal of Indian Business Research*, *7*(1), 67-102.

Bautista, J. R., Zhang, Y., & Gwizdka, J. (2022). Predicting healthcare professionals' intention to correct health misinformation on social media. *Telematics and Informatics*, *73*, 101864.

Bélanger, F., Collignon, S., Enget, K., & Negangard, E. (2017). Determinants of early conformance with information security policies. *Information & management*, *54*(7), 887-901.

Bokhari, S. A. A. (2023). A Quantitative Study on the Factors Influencing Implementation of Cybersecurity Laws and Regulations in Pakistan. *Social Sciences*, *12*(11), 629.

Bonnema, J. (2018). *5 reasons why your organization should adopt the NIST cybersecurity framework*. https://www.thesecurityawarenesscompany.com/2017/08/03/5-reasonsorganization-adopt-nist-cybersecurity-framework/

Boritz, J. E., Ge, C., & Patterson, K. (2022). Factors Affecting Employees' Susceptibility to Cyber-Attacks. *Journal of Information Systems*, *36*(3), 27-60.

Brown, E. (2016). Cybersecurity 'Rosetta Stone' celebrates two years of success.

Brownstein, J. S., Freifeld, C. C., Reis, B. Y., & Mandl, K. D. (2008). Surveillance Sans Frontieres: Internet-based emerging infectious disease intelligence and the HealthMap project. *PLoS medicine*, *5*(7), e151.

Business Partners Limited. (2022). *Cybercrime on the rise in SA: How to protect your business, customers and employees*. BizCommunity. Retrieved 25 April from https://www.bizcommunity.com/Article/196/841/230700.html

BusinessTech. (2022). *The world faces a cybercrime catastrophe - including South Africa*. Retrieved 25 April from https://businesstech.co.za/news/technology/639277/the-world-faces-a-cybercrime-catastrophe-including-south-africa/

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. *International journal of electronic commerce*, *9*(1), 70-104.

Celik, H. (2008). What determines Turkish customers' acceptance of internet banking? *International journal of bank marketing*, *26*(5), 353-370.

Cheung, M. F., & To, W.-M. (2016). Service co-creation in social media: An extension of the theory of planned behavior. *Computers in human behavior*, *65*, 260-266.

Chipeta, E. M. (2019). *Antecedents of social entrepreneurial intentions among Generation Y university students in South Africa* North-West University (South Africa). Vanderbijlpark Campus].

Choejey, P., Murray, D., & Fung, C. C. (2016). Exploring Critical Success Factors for Cybersecurity in Bhutan'S Government Organizations. Eighth International Conference on Networks & Communications,

Chu, S.-C., Chen, H.-T., & Sung, Y. (2016). Following brands on Twitter: An extension of theory of planned behavior. *International Journal of Advertising*, *35*(3), 421-437.

Cisco. (2023). *What is a Cyberattack*. Retrieved 25 April from https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html

Clark, L. A., & Watson, D. (2019). Constructing validity: New developments in creating objective measuring instruments. *Psychological assessment*, *31*(12), 1412.

Cohen, J., Cohen, P., West, S. G., & Aiken, L. S. (1983). Applied multiple regression. *Correlation Analysis for the Behavioral Sciences*, *2*.

Creswell, J. W., & Creswell, J. D. (2018). *Research Design Qualitative, Quantitative, and Mixed Methods Approaches* (Vol. Fifth Edition). SAGE Publications.

D'Arcy, J., & Hovav, A. (2007). Deterring internal information systems misuse. *Communications of the ACM*, *50*(10), 113-117.

Darem, A. A., Alhashmi, A. A., Alkhaldi, T. M., Alashjaee, A. M., Alanazi, S. M., & Ebad, S. A. (2023). Cyber threats classifications and countermeasures in banking and financial sector. *IEEE Access*, *11*, 125138-125158.

Dasgupta, D., Akhtar, Z., & Sen, S. (2022). Machine learning in cybersecurity: a comprehensive survey. *The Journal of Defense Modeling and Simulation*, *19*(1), 57-106.

Dash, M., Mohanty, A. K., Pattnaik, S., Mohapatra, R. C., & Sahoo, D. S. (2011). Using the TAM model to explain how attitudes determine adoption of internet banking. *European Journal of Economics, Finance and Administrative Sciences*, *36*(1), 50-59.

Davis, F. D. (1985). *A technology acceptance model for empirically testing new end-user information systems: Theory and results* Massachusetts Institute of Technology].

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS quarterly*, 319-340.

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User acceptance of computer technology: A comparison of two theoretical models. *Management science*, *35*(8), 982-1003.

De Vaus, D. (2001). Research design in social research. *Research design in social research*, 1-296.

Dedeke, A., & Masterson, K. (2019). Contrasting cybersecurity implementation frameworks (CIF) from three countries. *Information & Computer Security*, *27*(3), 373-392.

Deltour, F. (2012). ERP Project in SMEs: A matter of risks, a matter of competencies. A Quantitative analysis.

Denzin, N. K., & Lincoln, Y. S. (2011). *The Sage handbook of qualitative research*. sage.

Dholakia, U. M., & Soltysinski, K. (2001). Coveted or overlooked? The psychology of bidding for comparable listings in digital auctions. *Marketing Letters*, *12*, 225-237.

Dinev, T., & Hu, Q. (2007). The centrality of awareness in the formation of user behavioral intention toward protective information technologies. *Journal of the association for information systems*, *8*(7), 23.

Donaldson, S., E, Siegel, S., G, Williams, C., K, & Aslam, A. (2018). *Enterprise Cybersecurity Sudy Guide - How to Build a Successful Cyberdefense Program Against Advanced Threats*. Apress. https://doi.org/https://doi.org/10.1007/978-1-4842-3258-3

Egelman, S., & Peer, E. (2015). Scaling the security wall: Developing a security behavior intentions scale (sebis). Proceedings of the 33rd annual ACM conference on human factors in computing systems,

Enisa. (2018). Cybersecurity culture guidelines: behavioural aspects of cybersecurity. *European Union Agency for Network and Information Security*.

Eybers, S., & Mvundla, Z. (2022). Investigating cyber security awareness (CSA) amongst managers in small and medium enterprises (SMEs). Comprehensible Science: ICCS 2021,

Farooq, A., Ndiege, J. R. A., & Isoaho, J. (2019). Factors affecting security behavior of Kenyan students: an integration of protection motivation theory and theory of planned behavior. 2019 IEEE AFRICON,

Field, A. (2013). *Discovering statistics using IBM SPSS statistics*. sage.

FitzPatrick, B. (2019). Validity in qualitative health education research. *Currents in Pharmacy Teaching and Learning*, *11*(2), 211-217.

Gafni, R., & Pavel, T. (2019). The invisible hole of information on SMB's cybersecurity. *International Institute for Applied Knowledge Management*, *7*(1), 14 - 27.

Gale, M., Bongiovanni, I., & Slapnicar, S. (2022). Governing cybersecurity from the boardroom: challenges, drivers, and ways ahead. *Computers & Security*, *121*, 102840.

Gallaugher, J. (2011). *Information systems: A Manager's guide to harnessing technology*.

Ghafir, I., Prenosil, V., Hammoudeh, M., Aparicio-Navarro, F. J., Rabie, K., & Jabban, A. (2018). Disguised executable files in spear-phishing emails: Detecting the point of entry in advanced persistent threat. Proceedings of the 2nd International Conference on Future Networks and Distributed Systems,

Ghauri, P., Grønhaug, K., & Strange, R. (2020). *Research methods in business studies*. Cambridge University Press.

Goel, R., Kumar, A., & Haddow, J. (2020). PRISM: a strategic decision framework for cybersecurity risk assessment. *Information & Computer Security*, *28*(4), 591-625.

González-Granadillo, G., González-Zarzosa, S., & Diaz, R. (2021). Security information and event management (SIEM): analysis, trends, and usage in critical infrastructures. *Sensors*, *21*(14), 4759.

Gunduz, M. Z., & Das, R. (2020). Cyber-security on smart grid: Threats and potential solutions. *Computer networks*, *169*, 107094.

Hasanah, A. U., Shino, Y., & Kosasih, S. (2022). The Role Of Information Technology In Improving The Competitiveness Of Small And SME Enterprises. *IAIC Transactions on Sustainable Digital Innovation (ITSDI)*, *3*(2), 168-174.

Hasani, T., Rezania, D., Levallet, N., O'Reilly, N., & Mohammadi, M. (2023). Privacy enhancing technology adoption and its impact on SMEs' performance. *International Journal of Engineering Business Management*, *15*, 18479790231172874.

Hassan, A., Samy, G., Hegazy, M., Balah, A., & Fathy, S. (2024). Statistical analysis for water quality data using ANOVA (Case study–Lake Burullus influent drains). *Ain Shams Engineering Journal*, 102652.

Hassan, L. M., Shiu, E., & Shaw, D. (2016). Who says there is an intention–behaviour gap? Assessing the empirical evidence of an intention–behaviour gap in ethical consumption. *Journal of Business Ethics*, *136*, 219-236.

Hemant, P., Chawande, N. P., Sonule, A., & Wani, H. (2011). Development of servers in cloud computing to solve issues related to security and backup. 2011 IEEE International Conference on Cloud Computing and Intelligence Systems,

Henriksen, T. D., Nielsen, R. K., Vikkelsø, S., Bévort, F., & Mogensen, M. (2021). A paradox rarely comes alone a quantitative approach to investigating knotted leadership paradoxes in SMEs. *Scandinavian Journal of Management*, *37*(1), 101135.

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of information systems*, *18*, 106-125.

HM Government. (2016). National Cyber Security Strategy 2016-2021.

Hong, Y., & Furnell, S. (2022). Motivating information security policy compliance: Insights from perceived organizational formalization. *Journal of Computer Information Systems*, *62*(1), 19-28.

Hoong, Y., & Rezania, D. (2024). Balancing talent and technology: Navigating cybersecurity and privacy in SMEs. *Telematics and Informatics Reports*, *15*, 100151.

https://cybersecurityinstitute.co.za/academy/. (2024). *CSI Academy*. https://cybersecurityinstitute.co.za/academy/

Internet World Stats. (2021). *World Internet Usage and Population Statistics*. https://www.internetworldstats.com/stats.htm

Iuga, C., Nurse, J. R., & Erola, A. (2016). Baiting the hook: factors impacting susceptibility to phishing attacks. *Human-centric Computing and Information Sciences*, *6*, 1-20.

Jafarkarimi, H., Saadatdoost, R., Sim, A. T. H., & Hee, J. M. (2016). Behavioral intention in social networking sites ethical dilemmas: An extended model based on theory of planned behavior. *Computers in human behavior*, *62*, 545-561.

Jaruwachirathanakul, B., & Fink, D. (2005). Internet banking adoption strategies for a developing country: the case of Thailand. *Internet research*, *15*(3), 295-311.

Jung, J., Wang, V., & Kim, Y. (2020). South Korean Cyber Security Threats, Governance Measures, and Implications for SMEs. *Korean Journal of Industrial Security*, *10*(1), 81-109.

Jurgens, J. (2022). Preface. Cologny, Switzerland. *World Economic Forum*.

Kalidas, S., Magwentshu, N., & Rajagopaul, A. (2020). *How South African SMEs can survive and throve post COVID-19*. McKinsey & Company. https://www.mckinsey.com/featured-insights/middle-east-and-africa/how-south-african-smes-can-survive-and-thrive-post-covid-19#/

Kaspersky. (2023). *What is Cyber Security?* Retrieved 25 April from https://www.kaspersky.co.za/resource-center/definitions/what-is-cyber-security

Kim, H. L., Hovav, A., & Han, J. (2020). Protecting intellectual property from insider threats: A management information security intelligence perspective. *Journal of Intellectual Capital*, *21*(2), 181-202.

Kim, J.-O., & Mueller, C. W. (1978). *Introduction to factor analysis: What it is and how to do it*. Sage.

Kim, K., Youn, J., Yoon, S., Kang, J., Kim, K., & Shin, D. (2023). Study on Cyber Common Operational Picture Framework for Cyber Situational Awareness. *Applied Sciences*, *13*(4), 2331.

Kirlidog, M., van der Vyver, C., Zeeman, M., & Coetzee, W. (2018). Unfulfilled need: reasons for insufficient ICT skills in South Africa. *Information Development*, *34*(1), 5-19.

Kissel, R. (2013). Glossary of key information security terms, nistir 7298 revision 2. *Retrieved from National Institute of Standards and Technology website: http://nvlpubs. nist. gov/nistpubs/ir/2013/NIST. IR. 7298r2. pdf*.

Koigi, B. (2020). South Africa has third-highest number of cybercrime victims globally, report. *Africa Tech*, *4*.

Kondlo, A., Leenen, L., & van Vuuren, J. J. (2022). An Ontological Model for a National Cyber-Attack Response in South Africa. ECCWS 2022 21st European Conference on Cyber Warfare and Security,

Kraus, S., Rigtering, J. C., Hughes, M., & Hosman, V. (2012). Entrepreneurial orientation and the business performance of SMEs: a quantitative study from the Netherlands. *Review of Managerial Science*, *6*, 161-182.

Kumar, R., Sharma, S., Vachhani, C., & Yadav, N. (2022). What changed in the cyber-security after COVID-19? *Computers & Security*, *120*, 102821.

Kurpjuhn, T. (2015). The SME security challenge. *Computer Fraud & Security*, *2015*(3), 5-7.

Law, M. (2020). Continuance intention to use Facebook: understanding the roles of attitude and habit. *Young Consumers*, *21*(3), 319-333.

Lee, J., & Geistfeld, L. V. (1998). Enhancing consumer choice: Are we making appropriate recommendations? *Journal of Consumer Affairs*, *32*(2), 227-250.

Lee, Y., & Kozar, K. A. (2005). Investigating factors affecting the adoption of anti-spyware systems. *Communications of the ACM*, *48*(8), 72-77.

Lee, Y., Kozar, K. A., & Larsen, K. R. (2003). The technology acceptance model: Past, present, and future. *Communications of the association for information systems*, *12*(1), 50.

Li, P. P. (2007). Social tie, social capital, and social behavior: Toward an integrative model of informal exchange. *Asia Pacific Journal of Management*, *24*, 227-246.

Lomax, R. G., & Hahs-Vaughn, D. L. (2013). *Statistical Concepts-A Second Course*. Routledge.

Loo, M. K., Ramachandran, S., & Raja Yusof, R. N. (2023). Unleashing the potential: Enhancing technology adoption and innovation for micro, small and medium-sized enterprises (MSMEs). *Cogent Economics & Finance*, *11*(2), 2267748.

Lu, J., Wei, J., Yu, C.-s., & Liu, C. (2017). How do post-usage factors and espoused cultural values impact mobile payment continuation? *Behaviour & Information Technology*, *36*(2), 140-164.

Ma, X. (2022). IS professionals' information security behaviors in Chinese IT organizations for information security protection. *Information Processing & Management*, *59*(1), 102744.

Mabunda, S. (2021). Cybersecurity in South Africa: Towards Best Practices. In *CyberBRICS: Cybersecurity Regulations in the BRICS Countries* (pp. 227-270). Springer.

Malhotra, N., & Birks, D. F. (2007). An applied approach. *Marketing research. London: Prentice Hall*.

Malhotra, N. K. (2020). *Marketing research: an applied prientation*. pearson.

Malhotra, N. K., & Peterson, M. (2006). *Basic marketing research: A decision-making approach*. Prentice hall.

Malik, J. K., & Choudhury, S. (2019). Cyber Space-Evolution and Growth. *East African Scholars Journal of education, Humanities and Literature*, *2*(3).

Mallick, M. A. I., & Nath, R. (2024). Navigating the Cyber security Landscape: A Comprehensive Review of Cyber-Attacks, Emerging Trends, and Recent Developments. *World Scientific News*, *190*(1), 1-69.

Mashiane, T., & Kritzinger, E. (2021). Identifying behavioral constructs in relation to user cybersecurity behavior. *Eurasian Journal of Social Sciences*, *9*(2), 98-122.

Mcanyana, W., Brindley, C., & Seedat, Y. (2020). Insight into the cyberthreat landscape in South Africa. *Accenture*.

Miles, M. B., & Huberman, A. M. (1994). *Qualitative data analysis: An expanded sourcebook*. sage.

Mohit, H., Johnson, V. L., & Memarian Esfahani, S. (2023). Social media continuance from the perspective of commitment. *Journal of Computer Information Systems*, *63*(4), 904-918.

Mphatheni, M., Richard, & Maluleke, W. (2022). Cybersecurity as a response to combating cybercrime: Demystifying the prevailing threats and offering recommendations to the African regions. *International Journal of Research in Business & Social Sciences*, *11*(4), 384 - 396. https://doi.org/https://www.ssbfnet.com/ojs/index.php/ijrbs

Mun, Y. Y., & Hwang, Y. (2003). Predicting the use of web-based information systems: self-efficacy, enjoyment, learning goal orientation, and the technology acceptance model. *International journal of human-computer studies*, *59*(4), 431-449.

Murphy, C., Mtegha, C. Q., Chigona, W., & Tuyeni, T. T. (2022). Factors Affecting Compliance with the National Cybersecurity Policy by SMMEs in South Africa.

Murthy, S., & Bhojanna, U. (2009). *Business research methods*. Excel Books India.

Mzekandaba, S. (2024). *Cyber crime's annual impact on SA estimated at R2.2bn*. IT web. https://www.itweb.co.za/article/cyber-crimes-annual-impact-on-sa-estimated-at-r22bn/JN1gPvOAxY3MjL6m

Nafees, L., Cook, C. M., Nikolov, A. N., & Stoddard, J. E. (2021). Can social media influencer (SMI) power influence consumer brand attitudes? The mediating role of perceived SMI credibility. *Digital Business*, *1*(2), 100008.

National Institute of Standards and Technology. (2017). *Framework for Improving Critical Infrastructure Cybersecurity*. National Institute of Standards and Technology.

National Institute of Standards and Technology. (2018). Framework for improving critical infrastructure cybersecurity. *URL: https://nvlpubs. nist. gov/nistpubs/CSWP/NIST. CSWP*, *4162018*.

Ng, T. C., & Ghobakhloo, M. (2020). Energy sustainability and industry 4.0. IOP Conference Series: Earth and Environmental Science,

Ngoma, M. L., Keevy, M., & Rama, P. (2021). Cyber-security awareness of South African state-mandated public sector organisations. *Southern African Journal of Accountability and Auditing Research*, *23*(1), 53-64.

Olaitan, O. O., Issah, M., & Wayi, N. (2021). A framework to test South Africa's readiness for the fourth industrial revolution. *South African Journal of Information Management*, *23*(1), 1-10.

Paulsen, C., & Toth, P. (2016). *Small business information security: The fundamentals*.

Pawar, S., & Palivela, H. (2022). LCCI: A framework for least cybersecurity controls to be implemented for small and medium enterprises (SMEs). *International Journal of Information Management Data Insights*, *2*(1), 100080.

Philip, S. J., Luu, T. J., & Carte, T. (2023). There's No place like home: Understanding users' intentions toward securing internet-of-things (IoT) smart home networks. *Computers in human behavior*, *139*, 107551.

Pieterse, H. (2021). The cyber threat landscape in South Africa: A 10-year review. *The African Journal of Information and Communication*, *28*, 1-21.

Rahman, M., Ismail, I., & Bahri, S. (2020). Analysing consumer adoption of cashless payment in Malaysia. *Digital Business*, *1*(1), 100004.

Rahman, S., & Lackey, R. (2013). E-commerce systems security for small businesses. *International Journal of Network Security & Its Applications*, *5*(2), 193-210.

Rajab, M., & Eydgahi, A. (2019). Evaluating the explanatory power of theoretical frameworks on intention to comply with information security policies in higher education. *Computers & Security*, *80*, 211-223.

Rajivan, P., Moriano, P., Kelley, T., & Camp, L. J. (2017). Factors in an end user security expertise instrument. *Information & Computer Security*, *25*(2), 190-205.

Raosoft. (2004). *Sample Size Calculator*. http://www.raosoft.com/samplesize.html

Rau, P.-L. P., Gao, Q., & Ding, Y. (2008). Relationship between the level of intimacy and lurking in online social network services. *Computers in human behavior*, *24*(6), 2757-2770.

Rawindaran, N., Jayal, A., & Prakash, E. (2022). Exploration of the Impact of Cybersecurity Awareness on Small and Medium Enterprises (SMEs) in Wales Using Intelligent Software to Combat Cybercrime. *Computers*, *11*(12), 174.

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*, *3*(2), 100191.

Rogers, R. W., & Prentice-Dunn, S. (1997). Protection motivation theory.

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers & Security*, *53*, 65-78.

Saleem, J., Adebisi, B., Ande, R., & Hammoudeh, M. (2017). A state of the art survey-Impact of cyber attacks on SME's. Proceedings of the international conference on future networks and distributed systems,

Saleous, H., Ismail, M., AlDaajeh, S. H., Madathil, N., Alrabaee, S., Choo, K.-K. R., & Al-Qirim, N. (2023). COVID-19 pandemic and the cyberthreat landscape: Research challenges and opportunities. *Digital communications and networks*, *9*(1), 211-222.

Sánchez-Prieto, J. C., Olmos-Migueláñez, S., & García-Peñalvo, F. J. (2017). MLearning and pre-service teachers: An assessment of the behavioral intention using an expanded TAM model. *Computers in human behavior*, *72*, 644-654.

Sarmah, A., Sarmah, R., & Baruah, A. J. (2017). A brief study on cyber crime and cyber laws of India. *International Research Journal of Engineering and Technology (IRJET)*, *4*(6), 1633-1640.

Seacom. (2024). *What cyber threats are likely to entail in 2024*. https://seacom.co.za/news/what-cyber-threats-are-likely-to-entail-in-2024

Seyal, A. H., Noah Abd Rahman, M., & Awg Yussof Hj Awg Mohammad, H. (2007). A quantitative analysis of factors contributing electronic data interchange adoption among Bruneian SMEs: A pilot study. *Business Process Management Journal*, *13*(5), 728-746.

Shah, P. R., & Agarwal, A. (2020). Cybersecurity behaviour of smartphone users through the lens of fogg behaviour model. 2020 3rd International Conference on Communication System, Computing and IT Applications (CSCITA),

Sheeran, P., & Webb, T. L. (2016). The intention–behavior gap. *Social and personality psychology compass*, *10*(9), 503-518.

Shen, L. (2014). The NIST cybersecurity framework: Overview and potential impacts. *Scitech Lawyer*, *10*(4), 16.

Shingange, J. G. (2022). *Problematizing the South African cybersecurity policy landscape* Stellenbosch: Stellenbosch University].

Shropshire, J., Warkentin, M., & Sharma, S. (2015). Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *Computers & Security*, *49*, 177-191.

Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & management*, *51*(2), 217-224.

Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information management & computer security*, *8*(1), 31-41.

Sommestad, T., Karlzén, H., & Hallberg, J. (2017). The theory of planned behavior and information security policy compliance. *Journal of Computer Information Systems*.

Son, J.-Y. (2011). Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. *Information & management*, *48*(7), 296-302.

Song, J., Kim, J., & Cho, K. (2018). Understanding users' continuance intentions to use smart-connected sports products. *Sport Management Review*, *21*(5), 477-490.

Straub, D., Boudreau, M.-C., & Gefen, D. (2004). Validation guidelines for IS positivist research. *Communications of the association for information systems*, *13*(1), 24.

Sun, J., Sheng, D., Gu, D., Du, J. T., & Min, C. (2017). Understanding link sharing tools continuance behavior in social media. *Online Information Review*, *41*(1), 119-133.

Sürücü, L., & Maslakci, A. (2020). Validity and reliability in quantitative research. *Business & Management Studies: An International Journal*, *8*(3), 2694-2726.

Sutherland, E. (2017). Governance of cybersecurity-the case of South Africa. *The African Journal of Information and Communication*, *20*, 83-112.

Tam, T., Rao, A., & Hall, J. (2021). The good, the bad and the missing: A Narrative review of cyber-security implications for australian small businesses. *Computers & Security*, *109*, 102385.

Tan, G. W.-H., Chong, C.-K., Ooi, K.-B., & Chong, A. Y.-L. (2010). The adoption of online banking in Malaysia: an empirical analysis. *International Journal of Business and Management Science*, *3*(2), 169-193.

Teo, T. (2012). Examining the intention to use technology among pre-service teachers: An integration of the technology acceptance model and theory of planned behavior. *Interactive Learning Environments*, *20*(1), 3-18.

Tetteh, G. K., & Otioma, C. (2024). Cyberattack, cyber risk mitigation capabilities, and firm productivity in Kenya. *Small Business Economics*, 1-22.

Thakur, K., & Pathan, A.-S. K. (2020). *Cybersecurity fundamentals: a real-world perspective*. CRC Press.

Thaler, R. H., & Sunstein, C. R. (2008). Nudge: improving decisions about health. *Wealth, and Happiness*, *6*, 14-38.

Thompson, N., McGill, T. J., & Wang, X. (2017). "Security begins at home": Determinants of home computer and mobile device security behavior. *Computers & Security*, *70*, 376-391.

Todd, P., & Benbasat, I. (2000). Inducing compensatory information processing through decision aids that facilitate effort reduction: An experimental assessment. *Journal of Behavioral Decision Making*, *13*(1), 91-106.

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & management*, *49*(3-4), 190-198.

Veerasamy, N. M., Thulani; Mtsweni, Jabu. (2017). *A Baseline Study on CYbersecurity Readiness: A Report of the Department of Telecommunications and Postal Services*. D. o. T. a. P. Services.

Vorm, E., & Combs, D. J. (2022). Integrating transparency, trust, and acceptance: The intelligent systems technology acceptance model (ISTAM). *International Journal of Human–Computer Interaction*, *38*(18-20), 1828-1845.

Vrhovec, S., Bernik, I., & Markelj, B. (2023). Explaining information seeking intentions: Insights from a Slovenian social engineering awareness campaign. *Computers & Security*, *125*, 103038.

Wang, P., Liu, J., Zhong, X., & Zhou, S. (2023). A Cybersecurity Knowledge Graph Completion Method for Penetration Testing. *Electronics*, *12*(8), 1837.

Weickert, T. D., Joinson, A., & Craggs, B. (2023). Is cybersecurity research missing a trick? Integrating insights from the psychology of habit into research and practice. *Computers & Security*, *128*, 103130.

Whitman, M. E., & Mattord, H. J. (2021). *Principles of information security*. Cengage learning.

Whittaker, T. A., & Noteboom, C. (2019). Factors influencing curriculum adoption in undergraduate cybersecurity programs.

Wilson, M., McDonald, S., Button, D., & McGarry, K. (2023). It won't happen to me: surveying SME attitudes to cyber-security. *Journal of Computer Information Systems*, *63*(2), 397-409.

Wirth, A. (2019). Cyberinsights: Reviewing Today's Cyberthreat Landscape. *Biomedical Instrumentation & Technology*, *53*(3), 227-231.

Wong, L.-W., Lee, V.-H., Tan, G. W.-H., Ooi, K.-B., & Sohal, A. (2022). The role of cybersecurity and policy awareness in shifting employee compliance attitudes: Building supply chain capabilities. *International Journal of Information Management*, *66*, 102520.

World Economic Forum. (2023). *Global Cybersecurity Outlook 2023*.

Yiu, C. S., Grant, K., & Edgar, D. (2007). Factors affecting the adoption of Internet Banking in Hong Kong—implications for the banking sector. *International Journal of Information Management*, *27*(5), 336-351.

Yong, A. G., & Pearce, S. (2013). A beginner's guide to factor analysis: Focusing on exploratory factor analysis. *Tutorials in quantitative methods for psychology*, *9*(2), 79-94.

Yoon, C., Hwang, J.-W., & Kim, R. (2012). Exploring factors that influence students' behaviors in information security. *Journal of information systems education*, *23*(4), 407-416.

Yoon, H. S., & Steege, L. M. B. (2013). Development of a quantitative model of the impact of customers' personality and perceptions on Internet banking use. *Computers in human behavior*, *29*(3), 1133-1141.

Yudhiyati, R., Putritama, A., & Rahmawati, D. (2021). What small businesses in developing country think of cybersecurity risks in the digital age: Indonesian case. *Journal of Information, Commuication and Ethics in Society*, *19*(4), 446 - 462. https://doi.org/10.1108/JICES-03-2021-0035

APPENDIX A: PARTICIPATION INFORMATION SHEET

Dear Sir / Madam

My name is Jeeten Fakir and I am a Masters student (student number 2594644) at the University of the Witwatersrand, Johannesburg. My supervisor is Dr Eleanor Chipeta. I am conducting a research study about cybersecurity within the Small and Medium Business sector in South Africa.

The study title is: **An Investigation of Cybersecurity Implementation Challenges Among South African SMEs.**

I am inviting you to partake in my survey. If you decide to take part, your participation in this research study will last about 15-20 minutes. The research will take place at your convenience.

With your permission, I would like to use the data you provide to answer my research questions. This data will be stored on my locked laptop for 1 year. Only the researcher will have access to the data. The survey 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 or your business. 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 decide not to join. Taking part in the research study will not cost you anything.

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 afterward about this research study, feel free to contact me or my supervisor at 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), by telephone +27(0) 11 717 1408, email hrecnon-medical@wits.ac.za.

Yours sincerely,
Jeeten Fakir

Researcher:
Jeeten Fakir, 2594644@students.wits.ac.za, 0832121381

Supervisor
Eleanor Chipeta
0117178238
eleanor.chipeta@wits.ac.za

APPENDIX B: CONSENT FORM

Consent Form

Title of project: An investigation of cybersecurity implementation challenges among South African SMEs

Name of researcher: Jeeten Fakir

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 direct quotations from my survey 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 survey (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)

…… (signature)
…… (name of researcher/person seeking consent)
…… (date)

APPENDIX C: QUESTIONNAIRE

An Investigation of Cybersecurity Implementation Challenges Among South African SMEs

Start of Block: Default Question Block

Q1 Dear respondent,

My name is Jeeten Fakir, a Masters student (student number 2594644) at Wits Business School. I am conducting research on cybersecurity within SMEs, and the purpose of this study is to investigate cybersecurity awareness and implementation challenges among South African SMEs.

The survey will be confidential and anonymous. Your name or anything else that could identify you or your business will remain confidential. With your permission, I would like to use the data you provide to answer my research questions. This data will be stored on my locked laptop for one year. Only the researcher will have access to the data.

If you have any questions during or afterward about this research study, feel free to contact me (2594644@students.wits.ac.za / 083 212 1381) or my supervisor (eleanor.chipeta@wits.ac.za / 011 717 8238). 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), by telephone +27(0) 11 717 1408, email hrecnon-medical@wits.ac.za.

End of Block: Default Question Block

Start of Block: Block 1

Q2 **Subjective Norms and Beliefs Towards Cybersecurity**

Q3 Rate on a scale of 1 – 7 where: 1 = Strongly Agree, 2 = Agree, 3 = Slightly Agree, 4 = Neutral, 5 = Slightly Disagree, 6 = Disagree, 7 = Strongly Disagree

	1: Strongly Agree (1)	2: Agree (2)	3: Slightly Agree (3)	4: Neutral (4)	5: Slightly Disagree (5)	6: Disagree (6)	7: Strongly Disagree (7)
My business partners think that I should follow the information security policy (1)	○	○	○	○	○	○	○
My colleagues think that I should follow the information security policy (2)	○	○	○	○	○	○	○
Our IT department pressures me to follow its information security policy (3)	○	○	○	○	○	○	○
My subordinates think that I should follow the information security policy (4)	○	○	○	○	○	○	○

End of Block: Block 1

Start of Block: Block 2

Q4 **Attitude Towards Cybersecurity**

Q5 Rate on a scale of 1 – 7 where: 1 = Strongly Agree, 2 = Agree, 3 = Slightly Agree, 4 = Neutral, 5 = Slightly Disagree, 6 = Disagree, 7 = Strongly Disagree

	1: Strongly Agree (1)	2: Agree (2)	3: Slightly Agree (3)	4: Neutral (4)	5: Slightly Disagree (5)	6: Disagree (6)	7: Strongly Disagree (7)
The preventative measures available to me to stop people from gaining access to business information are adequate (1)	○	○	○	○	○	○	○
The preventative measures available to prevent people from causing damage to our information systems are adequate (2)	○	○	○	○	○	○	○
Following our information security policy is a good idea (3)	○	○	○	○	○	○	○
Following our information security policy is a necessity (4)	○	○	○	○	○	○	○

Following our information security policy is beneficial (5)	○	○	○	○	○	○	○
Following our information security policy is pleasant (6)	○	○	○	○	○	○	○

End of Block: Block 2

Start of Block: Block 3

Q6 **Perceived Behavioural Control**

Q7 Rate on a scale of 1 – 7 where: 1 = Strongly Agree, 2 = Agree, 3 = Slightly Agree, 4 = Neutral, 5 = Slightly Disagree, 6 = Disagree, 7 = Strongly Disagree

	1: Strongly Agree (1)	2: Agree (2)	3: Slightly Agree (3)	4: Neutral (4)	5: Slightly Disagree (5)	6: Disagree (6)	7: Strongly Disagree (7)
I have the necessary skills to protect my business from cybersecurity violations (1)	○	○	○	○	○	○	○
I have the expertise to implement preventative measures to stop people from accessing confidential business information (2)	○	○	○	○	○	○	○
I have the skills to implement preventative measures to stop people from damaging my work computer (3)	○	○	○	○	○	○	○
I believe that it is within my control to protect myself from cybersecurity violations (4)	○	○	○	○	○	○	○

I can enable cybersecurity measures on my company computer but only when I have manuals for reference (5)	○	○	○	○	○	○	○
For me, taking cybersecurity precautions is easy (6)	○	○	○	○	○	○	○
My ability to prevent cybersecurity breaches at my business is adequate (7)	○	○	○	○	○	○	○

End of Block: Block 3

Start of Block: Block 4

Q8 **Perceived Ease of Use of Cybersecurity Frameworks**

Q9 Rate on a scale of 1 – 7 where: 1 = Strongly Agree, 2 = Agree, 3 = Slightly Agree, 4 = Neutral, 5 = Slightly Disagree, 6 = Disagree, 7 = Strongly Disagree

	1: Strongly Agree (1)	2: Agree (2)	3: Slightly Agree (3)	4: Neutral (4)	5: Slightly Disagree (5)	6: Disagree (6)	7: Strongly Disagree (7)
Learning to operate cybersecurity tools and frameworks would be easy for me (1)	○	○	○	○	○	○	○
I would find it easy to get cybersecurity frameworks to work for my business (2)	○	○	○	○	○	○	○
My interaction with cybersecurity concepts and frameworks was clear and understandable (3)	○	○	○	○	○	○	○
I would find cybersecurity concepts and frameworks flexible to interact with (4)	○	○	○	○	○	○	○
It would be easy for me to become skilled in cybersecurity (5)	○	○	○	○	○	○	○
I would find cybersecurity concepts, techniques and frameworks easy to use (6)	○	○	○	○	○	○	○

End of Block: Block 4

Start of Block: Block 5

Q10 **Perceived Usefulness of Cybersecurity**

Q11 Rate on a scale of 1 – 7 where: 1 = Strongly Agree, 2 = Agree, 3 = Slightly Agree, 4 = Neutral, 5 = Slightly Disagree, 6 = Disagree, 7 = Strongly Disagree

	1: Strongly Agree (1)	2: Agree (2)	3: Slightly Agree (3)	4: Neutral (4)	5: Slightly Disagree (5)	6: Disagree (6)	7: Strongly Disagree (7)
Using cybersecurity tools and frameworks in my business would enable me to accomplish my business goals more quickly (1)	○	○	○	○	○	○	○
Using cybersecurity tools and frameworks would improve my businesses performance (2)	○	○	○	○	○	○	○
Using cybersecurity tools and frameworks in my job would increase my productivity (3)	○	○	○	○	○	○	○
Using cybersecurity tools and frameworks would enhance my effectiveness on the job (4)	○	○	○	○	○	○	○

Using cybersecurity tools and frameworks would make it easier to do my job (5)	○	○	○	○	○	○	○
I would find cybersecurity tools and frameworks useful in my business (6)	○	○	○	○	○	○	○

End of Block: Block 5

Start of Block: Block 6

Q12 **Academic, Professional Background, Computer Security Skills**

Q13 Do you have a degree in an IT-related field (e.g. information technology, computer science, electrical engineering, etc.)?

- ○ No (1)
- ○ Yes (2)

Q14 Have you ever taken or taught a course on computer security?

- ○ No (1)
- ○ Yes (2)

Q15 Is computer security one of your primary job responsibilities?

- No (1)
- Yes (2)

Q16 Have you attended a computer security conference in the past year?

- No (1)
- Yes (2)

Q17 Have you ever installed a computer programme?

- No (1)
- Yes (2)

Q18 Have you ever written a computer programme?

- No (1)
- Yes (2)

Q19 Have you ever designed a website?

- No (1)
- Yes (2)

Q20 Have you ever registered a domain name?

- No (1)
- Yes (2)

Q21 Have you ever created a database?

- No (1)
- Yes (2)

Q22 Have you ever used SSH to encrypt data?

- No (1)
- Yes (2)

Q23 Have you ever configured a firewall?

- No (1)
- Yes (2)

End of Block: Block 6

Start of Block: Block 7

Q24 **Demographics**

Q25 Age

- Below 18 years (1)
- 18 - 20 years (2)
- 21 - 30 years (3)
- 31 - 40 years (4)
- 41 - 50 years (5)
- 51 - 60 years (6)
- 61+ years (7)

Q26 Gender

- Male (1)
- Female (2)
- Prefer not to say (3)

Q27 Nationality

- South African (1)
- Anther African Country (2)
- Other (3)

Q28 Race

- Black (1)
- White (2)
- Coloured (3)
- Indian (4)
- Other (5)

Q29 Highest level of education

- ○ Matric (1)
- ○ Certificate (2)
- ○ Diploma (3)
- ○ Undergraduate degree (4)
- ○ Postgraduate degree (5)
- ○ Masters (6)
- ○ PhD (7)

Q30 Field of study

- ○ IT (1)
- ○ Engineering (2)
- ○ Commerce (3)
- ○ Humanities (4)
- ○ Other (5)

Q31 Number of employees

- ○ 1 - 5 (1)
- ○ 6 - 20 (2)
- ○ 21 - 50 (3)
- ○ 51 - 100 (4)
- ○ 100+ (5)

Q32 Industry

- Retail (1)
- Financial Services (2)
- Telecommunications and ICT (3)
- Healthcare (4)
- Mining (5)
- Agriculture (6)
- Logistics (7)
- Fashion (8)
- Digital Commerce (9)

End of Block: Block 7

APPENDIX D: ETHICS CLEARANCE CERTIFICATE

Graduate School of Business Administration
University of the Witwatersrand, Johannesburg

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

Ethics Clearance Certificate

Ethics protocol number: WBS/DB2594644/540
This certificate is only valid with a legitimate ethics protocol number and signed by the Researcher (below).

Project title	An Investigation of Cybersecurity Awareness and Implementation Challenges Among South African SME Owners
Investigator / Researcher	Mr Jeeten Fakir
Nature of Project	MM (Digital Business)
Decision of the Committee	Approved, provided stakeholders and participants are guaranteed confidentialty.
Issue Date of Certificate	17/08/2023
Expiry date	Date of submission of the project / research report
Chairperson	Dr Pius Oba ☎ +27 11 717 3976 +27 82 733 6587 ✉ pius.oba@wits.ac.za

Declaration by Researcher

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

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

Signature _____ Date: _____