



Examining factors influencing business perceptions of online privacy and security risk in Central South Africa

XA Boqo

 **orcid.org/0000-0006-7546-4741**

Mini-dissertation accepted in partial fulfilment of the requirements for the degree *Master of Business Administration* at the North-West University

Supervisor: Mr. JC Coetzee

Graduation: November 2025

DECLARATION

I, Xolani Boqo, declare that the research study titled “Examining Factors Influencing Business Perceptions of Online Privacy and Security Risk in Central South Africa” is my unique creation. This work has been presented as part of the criteria for obtaining a Master of Business Administration (MBA) degree at the North-West University Business School.

I assert that this research has not been presented before by anyone else or me to earn a degree or certification from any university or educational establishment. All references to information sources utilised or cited in this work have been appropriately acknowledged through citations following the North-West University (NWU) Harvard style referencing guidelines.

I confirm that I have followed the guidelines of academic research by diligently protecting the privacy and confidentiality of all participants in my study without any conflicts of interest during its execution under the guidance of my supervisor, Mr. JC Coetzee.

Name: Xolani Aubrey Boqo

Student number: 28744780

ACKNOWLEDGEMENTS

I want to start by saying thanks to my mother, Landiwe Florence Boqo for always being there for me and for her support and love during this journey. I am deeply grateful for her belief in me and all the sacrifices she has made while having faith in my capabilities throughout these times.

My heartfelt gratitude goes to all the professors and staff at the Business School for guiding and supporting me throughout this research journey with their expertise and encouragement.

I would also like to thank my supervisor, Mr. J.C. Coetzee, for his expertise and guidance during this research project. His feedback has been constructive. I appreciate his patience and dedication in helping me succeed. His mentorship means a lot to me.

A big thank you to all those who have been with us throughout this journey; your support and motivation have made this accomplishment a reality.

I want to thank the Greater Force for being with me and providing guidance and support during this adventure's ups and downs.

To all the participants involved in the study, a heartfelt thank you, as well as to the entrepreneurs who generously shared their insights.

ABSTRACT

The rapid expansion of e-commerce in central South Africa has increased the importance of privacy and security issues for medium-sized enterprises. However, there remains a dearth of information on how business managers perceive and react to such matters. The purpose of this study is to examine the factors that influence how small and medium-sized enterprises (SMEs) in Central South Africa perceive online privacy and security risks. The purpose of the study is to pinpoint and examine the major factors that influence these perceptions, including organizational culture, managerial awareness, technology preparedness and regulatory environment. By doing this, the study seeks to improve knowledge of how SMEs perceive and react to online privacy and security issues, offering insights that can guide better approaches to controlling and reducing digital risks in the area. The study was underpinned by the Theory of Planned Behavior (TPB), Protection Motivation Theory (PMT) and the Technology Acceptance Model (TAM). These frameworks collectively guided the understanding of behavioural intentions, motivational processes and technology adoption in the study context. Thirteen managers and business owners from a variety of industries, including IT, retail, manufacturing, construction and consulting participated in semi-structured interviews to gather data. This study sought to examine how risk management practices are influenced by peer networks, infrastructure dependencies and adaptive learning.

The results show that depending on cloud services from outside sources typically carries extremely high legal and geopolitical risks, which causes jurisdictional anxiety among medium-sized enterprises. Cybersecurity knowledge in central South Africa is primarily acquired through experience and anecdote-based word of mouth, rather than through formal education. This has resulted in skilled but technically limited responses. Medium-sized enterprises in central South Africa demonstrate a high level of awareness of reputational risk and apply data minimisation practices to maintain client trust. This indicates self-regulation in situations of weak local regulation.

The study highlights the interplay between infrastructural constraints, cultural issues and the availability of cybersecurity knowledge in influencing the responses of enterprises to privacy and security risks. It recommends that policymakers, local government authorities and development agencies implement targeted education and policy interventions to

enhance resilience among SMEs in semi-urban economies, while also recognising the value of grassroots learning and adaptive governance in the local context.

Keywords: Security risks, Central South Africa, small and medium-sized enterprises, Online privacy, Digital transformation, General Data Protection Regulation, Protection of Personal Information Act.

LIST OF ABBREVIATIONS

B2B	Business-to-Business
B2C	Business-to-Consumers
CSA	Central South Africa
CRM	Customer Relationship Management
FS	Free State
GDP	Gross Domestic Product
GDPR	General Data Protection Regulation
IT	Information Technology
NC	Northern Cape
NW	North West
POPIA	Protection of Personal Information Act
PMT	Protection Motivation Theory
RBV	Resource-Based View
SA	South Africa
Stats SA	Statistics South Africa
SMEs	Small and Medium-sized Enterprises
TAM	Technology Acceptance Model
TPB	Theory of Planned Behaviour

TABLE OF CONTENTS

DECLARATION	I
ACKNOWLEDGEMENTS	II
ABSTRACT	III
LIST OF ABBREVIATIONS	V
CHAPTER 1: NATURE AND SCOPE OF THE STUDY.....	1
1.1 INTRODUCTION	1
1.2 BACKGROUND OF THE STUDY	2
1.3 DEFINITION OF TERMS	3
1.4 PRELIMINARY LITERATURE REVIEW.....	7
1.4.1 Online privacy and security.....	8
1.4.2 Theoretical perspectives that inform business perceptions of online privacy and security	8
1.4.3 Internet privacy and security in South African SMEs features of CSA's SMEs.....	9
1.4.4 Contextual and psychological drivers influencing SME managers' views on privacy and security threats	9
1.4.5 Research Gap	10
1.5 PROBLEM STATEMENT	10
1.6 RESEARCH AIM AND OBJECTIVES	12
1.6.1 PRIMARY OBJECTIVE	12
1.6.2 SECONDARY OBJECTIVE	13
1.7 SCOPE OF THE STUDY AND DELIMITATIONS	13
1.8 RESEARCH METHODOLOGY	15

1.9	ETHICAL CONSIDERATIONS.....	30
1.10	ETHICAL PROTOCOLS	30
1.11	CHAPTER SUMMARY.....	33
1.12	THE LAYOUT OF THE STUDY.....	35
1.13	Conclusion.....	36
1.14	Chapter Summary.....	36
	CHAPTER 2: LITERATURE REVIEW	38
2.1	INTRODUCTION	38
2.2	THEORETICAL FRAMEWORK	40
2.2.1	Technology Acceptance Model (TAM)	41
2.2.2	Theory of Planned Behaviour (TPB)	41
2.2.3	Protection Motivation Theory (PMT)	42
2.2.4	Relevance to the current study	42
2.3	REVIEW OF CRITICAL THEMES AND TOPICS	43
2.3.1	Risks associated with online privacy and security in business conditions	43
2.3.2	Factors influencing how businesses view privacy and security risks	44
2.3.3	The impacts of privacy and security risks on business functions.....	44
2.3.4	Approaches utilised by businesses to address online privacy and security risks.....	44
2.3.5	The influence of frameworks on how businesses perceive and handle online privacy and security matters.....	45
2.3.6	Gaps in the literature	45
2.4	CRITICAL ANALYSIS OF REVIEWED LITERATURE.....	46

2.4.1	Strength of the existing literature	46
2.4.2	Limitations of existing literature.....	47
2.4.3	Areas where the literature is robust	47
2.4.4	Areas where the literature is lacking	48
2.4.5	How will the research build upon or challenge the existing literature.....	48
2.5	CONCLUSIONS	49
CHAPTER 3: EMPIRICAL STUDY		51
3.1	INTRODUCTION	51
3.2	Demographic characteristics of participants	51
3.3	Themes.....	57
3.3.1	3.3.1 Theme 1: Underlying influences on business perceptions.....	57
3.3.2	3.3.2 Theme 2: Perceived risk in e-commerce and online business environments.....	60
3.3.3	Theme 3: Leadership knowledge and adaptive security practices.....	62
3.3.4	Theme 4. Cultural and political contexts of trust.....	65
3.3.5	Theme 5: Sentiment and emotional orientation to risk	67
3.3.6	Theme 6: Tactical innovation and future-ready solutions	70
3.4	Summary	73
CHAPTER 4: CONCLUSION AND RECOMMENDATIONS		74
4.1	Introduction	74
4.2	Summary of key findings	74
4.3	Conclusion.....	76
4.4	Recommendations.....	76

4.4.1	Contextual, visual policy tool development	76
4.4.2	Local hosting and infrastructure development.....	77
4.4.3	Strengthening peer-led cybersecurity training	77
4.4.4	Including cybersecurity in business support curricula.....	78
4.4.5	Building innovation ecosystems through local developer forums	78
4.4.6	Promoting cybersecurity through public awareness campaigns	79
4.5	Achievement of study objectives	79
4.6	Contribution of the Study.....	82
4.6.1	Contribution to Policymakers	82
4.6.2	Contribution to small and medium-sized enterprises.....	82
4.6.3	Contribution to literature	82
4.7	Limitations of the study	84
4.8	Suggestions for future studies	84
	REFERENCE LIST	86
	ANNEXURE A: INFORMED CONSENT LETTER	102
	ANNEXURE B: LETTER OF GOODWILL.....	104
	ANNEXURE C: PERMISSION TO CONDUCT INTERVIEWS LETTER.....	106
	ANNEXURE D: DATA COLLECTION TOOL	108
	ANNEXURE E: ETHICS APPROVAL LETTER	111
	ANNEXURE F: LANGUAGE EDITING CERTIFICATE	112

LIST OF TABLES

Table 3.1. Demographic characteristics of the participants.....	52
Table 3.2. Alignment of themes with the research objectives	54
Table 4.1. Achievement of study objectives.....	80

LIST OF FIGURES

Figure 1. Map of Central South Africa.....	6
Figure 2. The research onion.....	16
Figure 3. Themes generated from the research objective.....	57
Figure 4. Themes that emerged from the research objective	60
Figure 5. Themes that emerged from the research objective: Investigate the extent of comprehension and awareness of privacy/security principles	62
Figure 6. Themes that emerged from the research objective: Assess how cultural forces affect the way managers view and feel about privacy and security.....	65
Figure 7. Themes that emerged from the research objective: review opinions and concerns about privacy/security	68
Figure 8. Themes that emerged from the research objective: Propose tactics to improve security/privacy protocols	70

CHAPTER 1: NATURE AND SCOPE OF THE STUDY

1.1 INTRODUCTION

Today, the issues surrounding privacy and security are of growing importance (Hiranandani, 2011:23). The rise of online shopping and internet activities has brought challenges and opportunities in areas such as Central South Africa (CSA), where there is a thriving online market (Mkhize, 2022:56). Although current studies have focused mainly on understanding how small and medium-sized enterprise (SME) managers perceive risks related to privacy and security, there is still a gap in understanding how businesses and managers of online platforms view and address these risks (Xue *et al.*, 2020:123; Gupta & Arora, 2019a:74).

CSA business operations are witnessing a rise in the utilisation of the internet and associated technologies. The growing trend is evident through the surge in transactions between businesses and SME managers as highlighted by the International Trade (Administration, 2024). Along with this transition in business practices, e-commerce emphasises the significance of exploring how companies perceive the risks linked to online privacy and security, as INTERPOL (2025) noted. Nevertheless, as firms adopt platforms for their transactions and interactions, they are also encountering increasing challenges such as cybersecurity threats, identity theft issues and breaches of privacy as discussed by Jones (2023).

This research aims to address this gap by investigating how companies in CSA perceive privacy and security threats. CSA is chosen due to its special economic setting and the various types of enterprises that offer invaluable insights into regional variations in attitudes towards privacy and security. Although it would be perfect to cover the perspective of the entire country, limiting it to parts of the CSA results in a deeper analysis that is within the scope of this investigation. By understanding the factors that shape these views, the study aims to offer insights for crafting strategies to reduce risks and bolster security protocols in business settings. In addition, this study aims to improve the understanding of how technology, business strategies and cybersecurity are affected in the changing environment of CSA.

The diverse range of factors that affect how businesses perceive privacy and security risks requires a multifaceted research approach (Liu & Babar, 2024). This investigation will explore elements, such as how security and privacy concerns affect business behaviours, attitudes and risk management tactics (Liu & Babar, 2024). Through an analysis of these aspects, the study aims to present a framework for understanding and tackling the obstacles encountered by businesses operating in the landscape, in CSA.

In conclusion, this study is essential both for addressing privacy and security challenges and for businesses and policymakers seeking to understand these challenges. By exploring the factors that affect how businesses view CSA, this research strives to help create strategies that protect businesses and SME managers worldwide.

1.2 BACKGROUND OF THE STUDY

Globally, threats to privacy and security have grown with the accelerating pace of digitalization of business operations. Cybercrime has become one of the biggest threats to economic stability, with global damages are projected to surpass USD 10 trillion annually by 2025 (World Economic Forum, 2024). In the majority of developing economies, like those of CSA, weak regulatory enforcement, low cybersecurity infrastructure and inadequate data protection regulations heighten these risks (African Union, 2023). South Africa has made progress with the enactment of the Protection of Personal Information Act (POPIA) of 2013, although the majority of small and medium enterprises (SMEs) continue to struggle with compliance as a result of limited technical capacity and awareness (Madisha & Kalema, 2022).

These comprise the utilisation of outdated software, weak data-management practices, poor encryption and lack of skilled IT personnel, elements that leave online businesses vulnerable to high levels of data breaches, phishing and identity theft. In the CSA region, these vulnerabilities are worsened by poor infrastructure, unstable internet connectivity and the high cost of cybersecurity tools. SME managers' perceptions of privacy and security risks are shaped by their past experiences with cyberattacks, level of trust in digital platforms, organisational capacity and confidence in government protection measures (Mugwagwa *et al.*, 2024). Collectively, these observations underscore the necessity of focused interventions to promote cybersecurity awareness, build digital resilience and strengthen legal and institutional arrangements across the region.

In the heart of Southern Africa (SA), businesses are navigating the growing world of online shopping, which presents both obstacles and opportunities for growth (Chen *et al.*, 2019b:308). The increase in sales raises concerns about safeguarding privacy and ensuring security for companies interacting with consumers in a Business-To-Consumer (B2C) and Business-to-Business (B2B) context (Ilyoo & Hong, 2013a:185). In the realm of managers' behaviour and marketing studies, the connection between privacy perceptions and managers' actions has been explored. However, a distinct void exists in incorporating perspectives from computing or Information Technology (IT) fields (Kim & Park, 2017). This study sought to fill this void by shedding light on how security and risk elements affect the behaviours of businesses and SME managers in CSA.

SME in the area often struggle with a lack of IT knowledge and resources, leaving them exposed to cyber risks (Mugwagwa et al., 2024:1524). Although these businesses rely heavily on internet technologies for their operations, they encounter difficulties in identifying and managing security threats, according to the research by Ilyoo and Hong (2013b:929). Moreover, the limited availability of IT security experts worsens the cybersecurity situation, impeding the implementation of security measures (Price Waterhouse Coopers, 2008). This research focuses on SME in CSA to uncover the elements that affect how businesses view online privacy and security risks. The aim is to offer guidance for strengthening cybersecurity preparedness and building confidence in transactions.

1.3 DEFINITION OF TERMS

In this section, we provide definitions to help clarify the concepts used in the study. Understanding these concepts is crucial. The 'Definition of terms' section serves as a reference point to explain terminology or concepts that are utilised throughout the study.

E-commerce

Some people perceive e-commerce as trading, especially when perceived superficially. However, if one should delve deeper into the topic, as suggested by Chaffey and Ellis (2019:156), one will realise that it is a system that combines the vastness of the internet with commercial activities. These activities include not only buying and selling goods, but

also providing services and the critical transfer of data involved in these transactions (Hashemi-Pour & Lutkevich, 2023:10).

Perceptions of business

In this research, the term 'business perceptions' denotes the changing views and comprehension of privacy and security risks in company environments. According to Smith and Browne (2012:45), these perspectives are shaped by a range of elements such as history, industry stories and the changing digital realm.

Online privacy

According to Clarke (2010:45), online privacy goes beyond being an entitlement; it acts as a barrier to our digital realm. It is not about safeguarding our information from scrutiny, but also about upholding the authenticity of our online identity amidst various cyber risks.

Security risk

Using the terms 'firewalls' and 'antivirus software' might give the impression of understanding cybersecurity. According to experts such as Siponen and Vance (2010:487), cybersecurity goes beyond that. They explain cybersecurity as a concept that deals with disruptions that can jeopardise the security, accuracy and accessibility of data.

Central South Africa (CSA)

This research defines CSA as a specific geographical area, mainly in the Free State (FS) and extending into many parts of the North-West (NW) Province. This part is made up of major towns and cities that play a critical role in understanding the online retail platform management, business perceptions and data privacy issues in this region of the country.

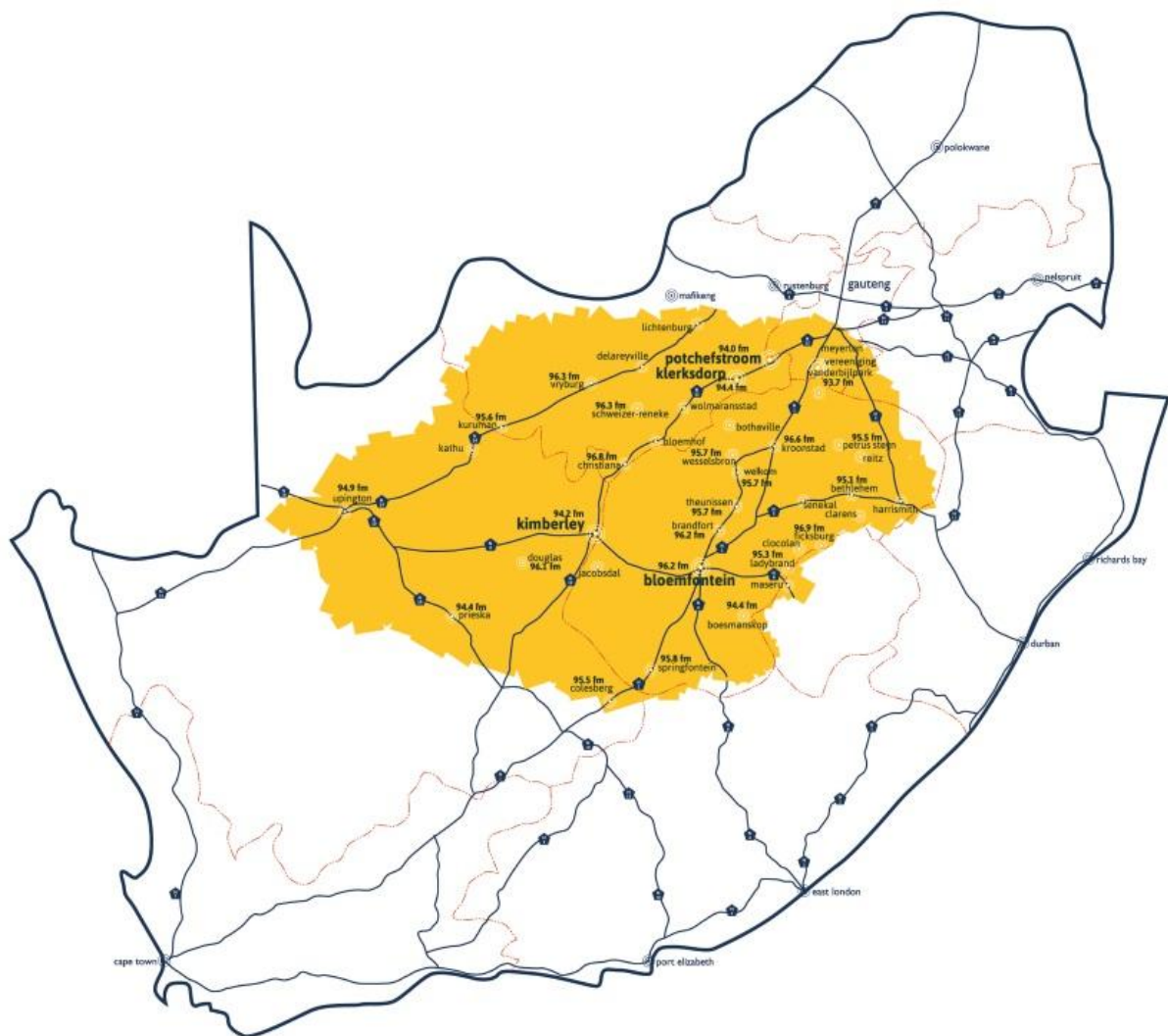
The research will be conducted in selected parts of the CSA, not throughout the entire CSA, which encompasses the FS, the NW, the Northern Cape (NC) and Gauteng. The researcher will cover different areas within this study area, namely:

1. **Bloemfontein:** This city is the capital of the FS and is often regarded as the judicial capital of South Africa (Government of South Africa, n.d.). It is essential as an

urban hub that contributes to the region's economy, culture and administration (Statistics South Africa, 2020).

2. **Sasolburg:** Sasolburg, located on the border between the FS and Gauteng, is renowned for its petrochemical sector and has a position in the local economy (South African Cities Network, 2016).
3. **Parys:** This charming settlement is located along the Vaal River and is renowned for its natural landscapes and a multitude of outdoor recreational pursuits (Free State Tourism, 2019).
4. **Kroonstad:** Agriculture and transportation play a role in this area of the FS, serving as an economic driver for the region (Free State Provincial Government, 2021).
5. **Potchefstroom:** Potchefstroom is in the NW. It has been included in the research because of its importance as a hub with notable commercial operations (North West University, 2020).
6. **Klerksdorp:** This is another crucial urban centre in the NW and is recognised for its mining and manufacturing sectors (South African Cities Network, 2018).
7. **Kimberley:** This city in the NC is famous for its history and diamond mining sectors (Northern Cape Tourism Authority, 2020).
8. **Vanderbijlpark:** Vanderbijlpark, located in Gauteng, is recognised for its steel manufacturing and industrial sectors (Gauteng Provincial Government, 2017).
9. **Lichtenburg:** This town is located in the NW and is famous for its agricultural operations and cement manufacturing (North West provincial government, 2019).

Figure 1. Map of Central South Africa



Source: OFM, n.d.

Trustworthiness of online business platforms

Building trust in online shopping platforms is essential for gaining the trust of users in regions like the CSA, where digital skills and economic backgrounds vary, which influences how people shop online (Hashemi-Pour & Lutkevich, 2023:25). This hinges on elements like the trustworthiness and dependability of these platforms, which provide users with the assurance that their transactions are safe and that their requirements are addressed.

Protection of Personal Information Act (POPI Act)

According to Kritzinger and Smith (2021a:5), the Protection of Personal Information Act (POPI Act) is more than just a regulation. It signifies a plea for data protection in CSA to establish a norm and advise retailers on how to build trust with users.

Loyalty

In the world of technology as Hartman (2015:12) points out, loyalty goes beyond repeat business. It encompasses a balance of trust, satisfaction and perceived value that compels managers of SME to repeat business, even in the face of tempting offers from rival companies.

Influencing

‘Influencing’ is the skill of shaping how people perceive and act in the era of digital technology. In the same way that a puppeteer is the force that controls the puppet, influencers are steering choices and viewpoints among managers without the users realising it (Black, 2018:36).

Regulatory environment

As discussed by Patel and Singh (2020:61), a regulatory environment goes beyond a collection of regulations. Instead, it represents an evolving environment that governs behaviour, guaranteeing that the digital world is not akin to the untamed Western frontier, but instead has its refined code of morals.

1.4 PRELIMINARY LITERATURE REVIEW

Introduction to the review of the literature

A literature review analyses and explores the amount of information on a particular topic. It also helps identify gaps in existing research. In this study, the literature review is essential to investigating the aspects of privacy and security in SME located in CSA.

1.4.1 Online privacy and security

The revolution of business online has reshaped the concept of privacy and security in the global economy. Initially, online privacy entailed keeping one's personal or organisational data away from fraudulent use or misuse (Mou *et al.*, 2017:223). Over the years, the term has become broader. Now it encompasses more general cybersecurity practices like encryption, identity protection and compliance with data protection legislation. In our contemporary interconnected world, web security not only exists as a technical defence. It also encompasses a non-negotiable component in managerial decision-making that impacts trust, reputation and competitiveness. Therefore, privacy and security are understood as multifaceted concepts shaped by technology, governance systems and human behaviour (Nguyen & Huynh, 2022:112).

1.4.2 Theoretical perspectives that inform business perceptions of online privacy and security

How business managers perceive and respond to privacy and security risks on the web is influenced by a set of related theories. The present study draws on the Theory of Planned Behaviour (TPB), the Protection Motivation Theory (PMT) and the Technology Acceptance Model (TAM). Collectively, these theories offer behavioural, psychological and technological insights into how SME managers engage with online business systems.

The Theory of Planned Behaviour (TPB) posits that individuals' behaviour is driven by behavioral intentions to act, which are influenced by attitudes, social norms and perception of behavioural control (Ajzen, 1991). This theory in the online business environment depicts how managers' attitudes towards cybersecurity, perceived social norms and self-belief in their ability to implement safeguard mechanisms influence their online actions.

The Protection Motivation Theory (PMT) examine how individuals respond to threats perceived through cognitive evaluation and coping responses (Rogers, 1983). It focuses on two process threat appraisal (perceived vulnerability and severity) and coping appraisal (response efficacy and self-efficacy) that determine whether managers engage in preventive security behaviors such as more secure passwords, encryption or risk analysis.

Davis's Technology Acceptance Model (TAM, 1989) explains the way in which the usefulness and perceived ease of use drive individuals towards adopting technology. TAM finds application in SMEs in terms of understanding why some managers accept cybersecurity products and online transaction systems while others avoid such acceptance due to perceived complexity or mistrust.

These theories provide a conceptual framework from which the interrelation of perception, motivation and technology usage in SMEs can be explained. They will be discussed in detail throughout the main literature review chapter, where their concepts and empirical applications will be discussed further to position this research within the existing body of knowledge.

1.4.3 Internet privacy and security in South African SMEs features of CSA's SMEs

Small and medium enterprises (SMEs) in Central and Southern Africa (CSA) are critical to regional economic growth and employment. Their adoption of digital platforms for marketing, communication and transactions has grown over the past couple of years (Mokoena, 2019:4). However, despite being economically influential, the majority of SMEs do not have adequate cybersecurity infrastructure, making them susceptible to privacy intrusions and cyber fraud (Madisha & Kalema, 2022:58). The lack of financial resources, limited digital literacy and inadequate institutional support infrastructures enhance such vulnerabilities and subject SMEs to becoming easy prey to cybercriminals.

1.4.4 Contextual and psychological drivers influencing SME managers' views on privacy and security threats

The perceptions of managers on online privacy and security are influenced by a number of psychological and situational factors. The perceived effectiveness of government regulatory schemes, dependability of online sites, social pressure and awareness of cyber attacks all impact to some extent (Dlamini, 2016:45). Social and cultural settings also condition how managers view risk and trust technology. In South Africa, uneven enforcement of data protection law, unstable internet accessibility and sparse prevalence of low-cost cybersecurity software also shape such attitudes (Smith, 2021:78; Mugwagwa *et al.*, 2024:1524).

1.4.5 Research Gap

Despite a growing body of research that has examined online security and privacy, relatively less importance has been given to SMEs in CSA. The majority of the past studies have focused on large firms or consumer opinions without asking how the managers in SMEs perceive and manage cybersecurity risks when resources are limited. Moreover, despite theoretical frameworks such as TPB, PMT and TAM being widely used in technology adoption and risk behaviour research, their integration in the case of privacy and security perceptions among African SMEs remains under-researched. This study seeks to close such a gap by providing an empirically grounded and contextually relevant assessment of SME managers' perceptions of online privacy and security in the CSA region.

1.5 PROBLEM STATEMENT

In the heart of SA, a growing number of businesses are delving into online commerce to stay competitive and reach more customers. Yet, as these companies embrace the realm, business leaders are grappling with a question: *How do people perceive the risks associated with online security and privacy?* Understanding these perspectives is key to fostering trust and promoting the growth of SMEs in this region (South African Department of Trade and Industry, 2021; FinMark Trust, 2020).

For the past five years, SMEs in CSA have witnessed a notable 15% increase in sales after adopting e-commerce, indicating a shift towards digitalisation and online integration (South African Department of Trade and Industry, 2023:12). However, during this period there has also been a concerning 20% rise in reported cybersecurity incidents among this group (Cybersecurity SA, 2023:5). These contrasting statistics underscore a challenge of balancing progress with safeguarding online privacy and security.

The era of technology has undoubtedly reshaped the business environment, presenting opportunities, as well as obstacles. Establishing and maintaining trust in business is vital for dealings with the cornerstone of this trust rooted in safeguarding client data privacy and security (Smith, 2019b:45). For managers of SMEs, grasping these beliefs is more than just an information technology (IT) concern; it is a strategic imperative that can significantly influence their business direction.

Understanding and addressing concerns about online privacy and security become vital for SMEs, which often have fewer resources than large companies. This is because the failure to do so can result in a loss of trust in SME managers and damage their reputation in the current competitive digital market. In SA, there exists a complex combination of cultural, socioeconomic and technological factors that shape how SME managers perceive online privacy and security (Mkhize, 2020:23). However, there is a gap in qualitative research that explores this intricate mix from the point of view of managers in SMEs.

The aim of the research is therefore to fill this void by studying these perceptions in order to make recommendations to policymakers, local government authorities and development agencies to implement targeted education and policy interventions to enhance resilience among SMEs in semi-urban economies. The guide will help identify challenges and make recommendations on how best to build robust digital platforms capable of meeting the managers' expectations for security and privacy. The reason why it is essential is that it will assist in reducing cyber incidents, fostering business trust and ultimately enhancing sales, as well as brand reputation.

In SA, online privacy and security awareness are significant challenges for SMEs as they seek to grow while maintaining the trust of stakeholders and managers sustainably. In the presence of digital tools, these firms often have difficulty with limited resources and the expertise needed to enforce strong cybersecurity measures and broad-based data protection guidelines. As a result, they find it challenging to catch up with larger companies that possess more advanced technology and have greater financial resources.

The purpose of this research is to determine how SMEs in SA can navigate the complexities of internet privacy and safety beliefs to foster sustainable development while promoting business confidence in a fast-digitalising world. It will provide managers with essential insights that will help them develop trusted building strategies by identifying risks from the perspectives of SME managers.

Thus, the problem statement can be formulated as follows:

The significant challenges that businesses face in the digital domain in relation to managers' perceptions are what the research titled *“Examining Factors Influencing Business Perceptions of Online Privacy and Security Risk in Central South Africa”* is about. However, as SMEs in CSA progressively adopt digital channels into their business strategies, this study points out that business leaders are grappling with how to understand and manage online privacy and security risks. Many companies, despite knowing that they need strong security measures do not understand why certain elements affect the management attitude towards these risks. Therefore, this research aims to understand the factors that determine these views and to provide beneficial insights on improving cybersecurity practice, in addition to promoting trust in the SME setting.

Key refinements

1. **Conciseness and clarity:** The revised problem statement is more concise and focused than the original statement, thereby eliminating redundancy.
2. **Specificity:** The issue of balancing digital advancement with privacy and security concerns is specifically highlighted.
3. **Strategic importance:** It emphasises that SMEs must recognise these perceptions strategically.
4. **Practical application:** The practical applications of the research findings are clearly stated, indicating how business managers could use them for decision-making purposes.
5. **Contextual factors:** Discussing these perceptions recognises that they are underpinned by a unique mix of cultural, socioeconomic and technological factors in SA.

1.6 RESEARCH AIM AND OBJECTIVES

1.6.1 PRIMARY OBJECTIVE

The main objective of this study is to:

- Explore how managers in SMEs view privacy and security concerns on online shopping sites in the CSA region.

1.6.2 SECONDARY OBJECTIVE

- Exploring the perspectives of businesses in CSA that utilise e-commerce platforms on issues related to privacy and security.
- Investigate the extent of comprehension and awareness of security principles and privacy of businesses and SME managers across the selected regions.
- Assess how cultural forces affect the way business managers view and feel about online security and privacy.
- Explore strategies to enhance the comprehension and execution of security and privacy protocols in companies in the CSA region.

In conclusion, this study aims to improve our understanding of the factors that influence how SMEs perceive privacy and security risks in the CSA region, with a focus on businesses. Due to the challenges of reaching all managers of SMEs, the research will gather insights primarily from the perspective of platforms. Through achieving the objectives, this study intends to provide tailored insights to help SMEs navigate the complexities of managing privacy and security. The results of this study could potentially empower platforms in CSA by offering advice and methods to enhance their practices related to privacy and security, thus building trust in and credibility of the digital landscape.

1.7 SCOPE OF THE STUDY AND DELIMITATIONS

Field of Study

The research focused on examining how businesses in CSA perceive privacy and security risks. The investigation specifically targeted managers of SMEs to ensure consistency in the research findings. In the business domain, the study distinguishes between SMEs and large corporations. The varying budget constraints on security measures and potential interactions with partners of different sizes influence this choice. The research specifically targeted SMEs operating in CSA. This decision is based on the researcher's familiarity with the business landscape in this region and the limited access to these businesses compared to urban areas.

Sector under investigation

This research focused on the SME sector in CSA in the fields of IT and marketing management (Mkhize, 2020:56). The study delved into the challenges and opportunities that SMEs face in the landscape, investigating how online retail platform managers navigate the complexities of privacy and security (Kritzing & Smith, 2021b:8). These managers play a role in the economy of the region (Mkhize, 2020:63), so understanding their perspectives of these matters is crucial. By shedding light on the dynamics in this sector, this research aimed to provide information for developing strategies that build and maintain managers' trust, ensure compliance with emerging regulations (Kritzing & Smith, 2021a:10) and foster a secure online environment for users in CSA.

Geographical delimitation

This research is focused on CSA, considering the economic and social factors that contribute to perceptions of online relationships among SMEs. The unique blend of semi-urban environments in this area adds depth to the study, which allowed for the exploration of how digital adoption and online behaviour differ across various demographic segments, specifically in the SME sector. The primary focus of this research was on regions located in the CSA. The aim is to gain an understanding of the sociocultural and economic characteristics of the area, particularly in how SMEs engage.

- This study is a qualitative analysis, selected due to its proximity to the North-West University Business School, Potchefstroom campus making it easily accessible for the researcher to engage with the audience.
- To cover the entire territory of SA, a comprehensive approach would be required, which may include larger samples and a wide range of data collection, making the study too broad and complex. Consequently, by focusing on specific regions, the study achieved a more manageable and in-depth qualitative analysis.

Focusing on the FS and NW, the research aimed to delve into the heart of SA. This includes examining cities with significant online activity and rural areas that may show different online behaviours and perspectives. The primary goal was to gather data that

authentically reflects the population of SA and their digital involvement. To ensure an overview, the study encompassed towns including Bloemfontein, Sasolburg, Parys, Kroonstad, Potchefstroom, Klerksdorp, Kimberley, Vanderbijlpark and Lichtenburg.

1.8 RESEARCH METHODOLOGY

In the changing world of interactions, it is essential to grasp how companies in CSA view privacy and security risks. This part describes the plan and methods created to explore these aspects thoroughly. The strategy involves a research design aimed at revealing understandings considering the personal perspectives commonly held by businesses in this area. The study used qualitative methods to investigate the factors and mechanisms that influence the perceptions of SMEs regarding online privacy and security risks. A qualitative approach was considered appropriate because it focuses on the in-depth investigation of perspectives rather than on the presentation of descriptions at the surface level. As Johnson and Christensen (2008) explained, qualitative research is useful at capturing phenomena and grasping interpretations within cultural contexts.

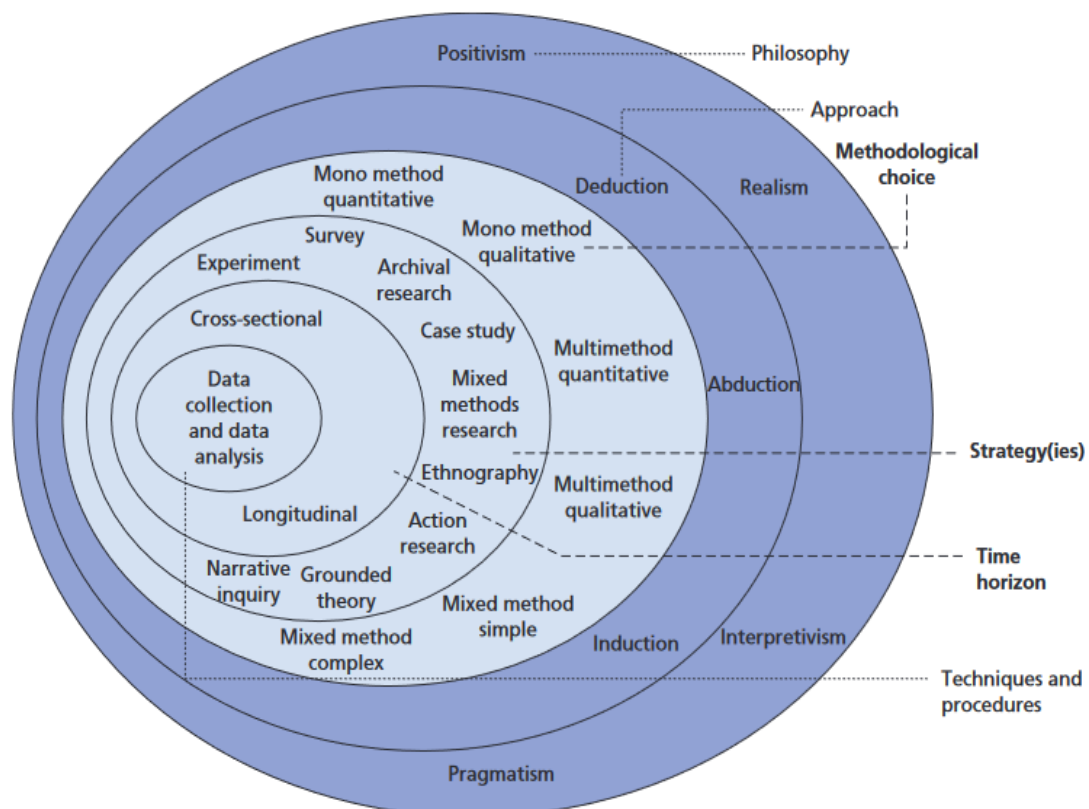
The core of the methodology lies in the use of semi-structured interviews to collect data. It is through a semi-structured interview where participants get to share their thoughts, feelings and fears regarding privacy and security risks. As per the extended approach recommended by Rubin and Rubin (2005), the interviews are designed in such a way that they enable free-flow discussions, while also ensuring that important issues are covered. The researcher conducted 15 virtual semi-structured interviews to gather rich responses and establish rapport. However, all interviews were done through electronic means, such as Microsoft Teams due to participant preferences, logistical challenges and health-related concerns as some indicated they were indisposed and did not wish to risk contracting the disease. These methods allowed participants to actively participate in the conversation actively, thereby providing insights into their opinions.

Additionally, the qualitative nature of the study allowed exploration of emerging themes and inconsistencies in the data. By maintaining adaptability in the interview process, unforeseen issues could be examined, enhancing comprehension of the business perspectives of privacy and security risks. This differs from methods where focus is often predetermined by researchers and confined to predefined categories. Moreover, considering the lack of research on this subject in the African setting, the study employed

a detailed interview methodology to gather detailed and descriptive information from businesses. This is in line with the suggestions of Creswell and Poth (2018:131), who support using specific techniques in investigating explored domains to produce thorough insights.

In general, the research method blends aspects of investigation, informal conversations and detailed data gathering to gain a grasp of the factors that shape how businesses perceive online privacy and security threats in CSA. This strategy is designed to uncover perspectives that can guide choices and support the creation of specific measures to address perceived risks in the online world.

Figure 2. The research onion



Source: Saunders *et al.* (2012:160)

Review of the literature

When starting the research journey, it is crucial to understand the existing knowledge related to the chosen topic. This initial phase is known as the literature review. During this process, researchers can explore perspectives on the subject, identify inconsistencies

and, importantly, recognise areas that have not been extensively studied yet (Meyer *et al.*, 2017:78). Specifically, for this study, the literature review thoroughly analysed aspects concerning how enterprises perceive online privacy and security risks with a specific focus on SMEs in CSA.

To understand the factors that affect these perceptions entirely in relation to SMEs, this study investigated a variety of sources. These sources include peer-reviewed articles from journals, online publications, previous dissertations, official reports, published materials and textbooks that explore the topics of privacy, security risks, business perceptions and the specific difficulties faced by SMEs in CSA. The main goal of this analysis was to enhance the understanding of aspects concerning how businesses, in CSA, perceive risks related to privacy and security. It sought to provide insights into the following topics.

- Delving into views on privacy. This includes examining the perspectives on internet privacy in the digital realm and grasping its importance for companies functioning in CSA.
- Understanding security threats in online transactions. This section aims to uncover and understand the security threats that businesses and their managers encounter when conducting transactions online. In addition, it seeks to assess how these risks have evolved.
- Exploring digital obstacles faced by enterprises. This part delves into the challenges that businesses and SMEs in CSA grapple with on a day-to-day basis.
- Analysing influential factors on business perspectives. This component involved an examination of the technological and organisational factors that influence how businesses perceive the risks associated with online privacy and security in the area.
- In this assessment, the focus is on revealing the approaches and top methods utilised by companies in CSA to reduce privacy and security threats while effectively handling SME managers' worries.

Through exploring these domains, this thorough examination not only lays the groundwork for studies, but also offers valuable perspectives and recommendations for

professionals and upcoming researchers in the realm of internet privacy and security in the business landscape of CSA.

Empirical study

- **Research paradigm**

In the current age of progress, it is crucial to understand how SMEs perceive and prioritise privacy and security. According to Van der Merwe *et al.* (2019:45), as online markets continue to grow in SA, it becomes essential to understand how SMEs navigate and perceive the virtual landscape. This is especially true in SA, where socioeconomic and cultural factors contribute to these different perspectives. Considering the subject at hand, this research followed the interpretive paradigm. According to Smith *et al.* (2021:56), this approach is most suitable when seeking to gain an understanding of individuals' subjective experiences and perceptions in an online setting. When it comes to examining the viewpoints of SMEs, this paradigm becomes crucial because experiences and cultural backgrounds inherently shape online risk and security perceptions.

Mokoena and Botha (2020:28) point out that in the South African SME sector, business perceptions vary significantly due to various factors such as historical disparities, levels of technological literacy and local cyber threats prevalent in their communities. By adopting an interpretive paradigm, the researcher ensured that he captured these perspectives comprehensively. In addition, it allowed the researcher to interact closely with participants on online platforms, resulting in a more nuanced understanding of the topic than would have been otherwise possible.

To address the issues faced by SMEs in SA regarding online privacy and security, the researcher directly interacted with representatives from a selected group of these enterprises. By engaging with enterprises, the researcher aimed to uncover the factors that influence their views on online privacy and security in the digital domain. By focusing on the perspectives of businesses, the researcher aimed to offer tailored insights and practical suggestions to address their distinct challenges and requirements in establishing digital trustworthiness (Khuzwayo, Petersen & Mthembu, 2018:22). To reach out to these enterprises, the researcher used various online communication platforms such as

Microsoft Teams, Zoom, WhatsApp and others to ensure easy and accessible participation for the participating businesses.

- **Research approach**

According to Smith and Johnson (2022:134), having a grasp of research paradigms is crucial for the researcher when it comes to making decisions about gathering and interpreting data. In the context of exploring the factors that influence business perceptions of online privacy and security risks in the SME sector of CSA, it is considered appropriate to use an inductive research approach. As defined by Smith and Johnson (2022:135), an inductive approach involves examining data, identifying patterns and drawing insights that can then lead to the development of theories or hypotheses. The main objective of this methodology is to collect data on how SA central businesses perceive online privacy. The goal is to draw conclusions that can be applied to the digital landscape of a SMEs (Parker *et al.*, 2020:403).

- **Methodological considerations**

The selection of the research methodology plays a role in shaping the direction and results of a study (Saunders *et al.*, 2009:583). In this investigation, the researcher uses a research approach to explore the factors that influence business perceptions of online privacy and security risk, specifically in the SME sector in CSA. Qualitative research is particularly effective in capturing the nuances of perspectives, emotions and personal experiences, which are essential for a topic deeply rooted in personal beliefs and experiences (Creswell, 2016:21). According to Bryman (2015:52), qualitative research allows us to understand how individuals construct their understanding of the world by examining the emergence of interconnectedness and the evolution of patterns and processes over time.

This research was primarily based on data collection through semi-structured interviews. These tools provide information to understand the factors that influence perceptions of online privacy and security in SMEs (Saunders *et al.*, 2010:491). The decision to use this approach was based on various reasons. First, the researcher aimed to gain insights into the experiences of SMEs in CSA regarding privacy and security risks. Since the study focused on SMEs and their unique cultural, socioeconomic and technological aspects, it

is crucial to capture these nuances. Furthermore, previous professional interactions with SMEs have given the researcher an understanding of the dynamics of the sector, further emphasising the need for a research design that can explore these intricacies. Furthermore, a qualitative approach aligns seamlessly with the objective of the study of understanding how SME managers express and interpret their experiences related to privacy and security risk. The qualitative approach was chosen for this study because it aligns with the researcher's goal of examining and understanding the factors that shape how SME managers perceive risks related to online privacy and security. This is particularly relevant in the context of the ecosystem of SMEs in CSA.

- **Research strategy**

To fully understand the factors that influence how businesses perceive privacy and security risks in SMEs in SA, it is essential to establish a precise research strategy. According to Smith *et al.* (2019:141), the choice of research strategy should align carefully with the research question, existing knowledge, time limitations, available resources and the fundamental philosophical principles that guide the study. As Brown and Anderson (2021:47) explain, descriptive research is beneficial for identifying attributes, frequencies, trends and connections within datasets. This approach holds promise for unravelling the factors involved in shaping perceptions of privacy and security among SMEs in CSA.

Using this research approach, the researcher aimed to collect information on how the managers of SMEs in CSA interact with other such companies online. Furthermore, this study aimed to understand concerns related to privacy and security and explore the factors that influence these perceptions. As stated by Smith *et al.* (2022:190), descriptive research provides a framework for identifying patterns, attitudes and behaviours without delving into the reasons behind them. This research focused on investigating how SMEs in CSA interact with their clients online. It emphasises the importance of gathering information through interviews with representatives from these enterprises to understand their strategies and obstacles in engaging with clients on digital platforms.

Furthermore, the research focuses on qualitative interviews to gain a deeper understanding of the dynamics between SMEs and their clients. This approach helps to uncover hidden aspects that quantitative methods may overlook. By exploring the perspectives of SMEs, the objective of the research is to reveal strategies and

opportunities to improve the trust of SME managers in interactions. This research strategy aims to provide SMEs with practical guidance on enhancing their online visibility and nurturing better connections with their managers. The emphasis here is on using interviews as the method for gathering data, focusing on understanding how SMEs engage with clients in the digital realm.

- **Study population and sample**

- A. Study Population

The study centres on businesses in CSA that are actively engaged in online commerce or digital platforms. This includes companies participating in endeavours such as selling goods online, digital advertising and interacting with managers on the internet. The main objective was to explore the view of these companies and address the challenges related to privacy and security. To determine the population size, the researcher collected data from sources such as Statistics South Africa (Stats SA) to establish how many SMEs are active in CSA. Based on that information, SA is home to 2.6 million SMEs, of which about 37% operate formally. Among these businesses, 54% are micro enterprises. The business owners come from a mix of people who seek business opportunities and those who run the enterprise out of necessity. Two-thirds of SME owners manage their businesses alone, while 32% provide job opportunities for one to ten (10) people. Despite varying growth rates, SMEs have contributed to South African value-added increase from 18% in 2010 to 40% in 2020 (Home, n.d.).

By defining the population and sample size, this study ensured the reliability and representation of its findings. Saunders *et al.* (2007:206) show that the population the researcher is interested in, involves all persons who own or manage SMEs and are familiar with privacy and security matters. Lastly, these data helped to determine a sample size following established methods and principles. First, prospective participants' contact details were obtained from CSA-specific public business directories and professional networks. Furthermore, the list of contacts obtained from these directories and networks was used after seeking permissions, thereby complying with the stipulated privacy regulations and ethical standards. As a result, this practice allowed the study to obtain a reliable and representative sample.

- B. Sampling frame

The sampling frame refers to the list of all population units from which the sample is drawn (Saunders *et al.*, 2007:208). For this research, the sampling frame included registered SMEs that are currently trading online in CSA. The businesses that were part of this sampling frame were identified through direct and indirect methods of communication and participation.

Direct methods:

- Reach out to industry associations.
- Consulting online directories.
- Accessing business registries.

Indirect methods:

- Recommendations from stakeholders or industry experts.
- Industry events and networking forums.

The sampling frame was designed to include businesses operating on the internet in CSA, using both direct and indirect approaches.

C. Inclusion and Exclusion Criteria

Inclusion criteria:

- SMEs operating online for at least three years.
- Businesses with a user base established on their online retail platforms.
- Companies which are managed directly by their owners.
- Companies located in the specific region of the CSA.

Exclusion criteria:

- SMEs without an online presence.
- Companies located outside of CSA, including the NW.
- Companies that have operated digitally for less than three years.

Clarification on geographic scope:

The study focuses on CSA, except for businesses in the NW and any other region outside this area. Only businesses in the CSA region are in the samples and populations to ensure a relevant and focused analysis of the target area.

D. Sample size

Sample size refers to the number of entities or observations that are part of the research. In this study, the researcher will use data saturation as a guideline to ensure an understanding of the factors that influence business perceptions. As explained by Saunders *et al.* (2018:1893), research saturation occurs when data no longer provide new insights. This study involved the owners and managers of 13 companies. However, data saturation was used to determine this sample size. Data saturation was reached after interviewing 13 participants. Data saturation indicates the point at which no new information or themes emerge from the data (Guest *et al.*, 2006:71). By including participants in this range, our goal is to gain insights into the factors that affect how businesses perceive privacy and security risks in CSA. This approach also ensures that we reach data saturation to maintain the credibility and accuracy of the research findings.

Therefore, evidence is that there are some 2.175 million privately owned businesses in SA, 2.15 million of which are SMEs. Of these, 1.5 million are not Value Added Tax (VAT) or Corporate Income Tax (CIT) registered and can therefore be classified as informal, 150,000 are SMEs, 450,000 are small businesses and 1.3 million are micro enterprises. As most estimates show that SMEs make up between 42 and 47 percent of the total employment of the country, significant growth in SMEs' contribution to Gross Domestic Product (GDP) is desirable. By 2030, small businesses will contribute 60-80% of GDP, accounting for 90% of the NDP's 11 million new jobs (Minister Lindiwe Zulu on the achievements of the Department of Small and Medium-sized Enterprises | Department of Small and Medium-sized Enterprises, 2017).

E. Sampling process

To ensure the precision and inclusiveness of the study, it is crucial to determine the population size before moving on to sampling. Drawing inspiration from Greener and Martelli (2018:68), who describe a sample as a subset that mirrors the population, the researchers will carefully determine the number of SME owners and managers involved

in online ventures in CSA. To gather data, this research used a snowball sampling interview approach as recommended by Cooper and Schindler (2014:360). This method uses existing participants to find respondents through a 'chain referral' process. Due to the challenges in accessing the target population, snowball sampling provides a way to recruit participants.

Moreover, this strategy is in line with the suggestions put forth by Saunders and colleagues (2019:245), particularly for groups with expertise, such as entrepreneurs. It is crucial to highlight the importance of following data protection laws, such as the Protection of Personal Information Act (POPI Act, 2019), throughout the study to ensure adherence and protect the privacy and confidentiality of the participants. Data collection continued until saturation was reached. Saturation occurs when no new insights emerge from the data and ensures an adequate sample size as emphasised by Creswell and Creswell (2018:301).

- Design of the measurement instrument

When studying factors that affect how business managers perceive online privacy and security risks about SMEs in CSA, it is essential to use appropriate data collection methods that are suitable for the research being conducted. Some tools can help gather a comprehensive understanding of SME managers' attitudes and behaviours towards online transactions (Smith & Johnson, 2016:150). Given the nature and complexity of the topic in the realm of SMEs, where approaches and protocols can vary firsthand, information was gathered directly from the participants via their accounts. These individuals, who have experience and perspectives, play a role in this study. However, it is essential to acknowledge that the quality of the data obtained through this method is based on the willingness of the participants to discuss their experiences openly.

To gather data for this research, given the nature and intricacy of the topic in the realm of SMEs, where approaches and protocols can vary firsthand, information will be collected directly from the participants through their accounts. At the time, it allows the researcher to steer the conversation in line with their research goals (Smith & Johnson, 2016:152). Moreover, by conducting semi-structured interviews, the researcher investigated situations where managers have had privacy concerns or faced security breaches. These real-life scenarios not only provided insights into the difficulties that SMEs face in

safeguarding security but also emphasised the steps they have implemented or can implement moving forward.

- Research instrument

Purpose:

The main research instrument for this study was a semi-structured interview guide. The guide was intended to collect qualitative data on factors that affect the perceptions of online privacy and security risks by SMEs in CSA. The semi-structured nature of interviews allows flexibility to investigate the participants' responses more deeply while maintaining coherence throughout the interviews (Creswell, 2014).

Construction to be measured:

Interview guides focus on the following key constructions:

1. Perceptions of online privacy risks: The participants were invited to describe their understanding and concerns about online privacy in their business activities.
2. Perceptions of online security risks: Questions explore how the participants perceive and manage online security threats in their businesses.
3. Impact on business decisions: This study examined how online privacy and security concerns influence business decisions and strategies.
4. Trust in online platforms: This guide explores the participants' trust in online platforms and tools used for business activities (Saunders *et al.*, 2016).
5. Experiences with privacy or security breaches: The participants were encouraged to share past experiences with privacy or security breaches and how these incidents affected their companies.

Reliability and validity:

In qualitative research, the reliability and validity of data collection devices are guaranteed by the following methods:

- Member verification: After the interview, the participants were given a summary of their responses to confirm the accuracy of the information collected (Birt *et al.*, 2016).
- Triangulation: The results of the interviews were examined with secondary data sources such as relevant literature and company documents to ensure coherence and credibility (Flick, 2018).
- Reflexivity: Researchers maintain reflective journals to document and minimise potential biases affecting data collection and analysis (Berger, 2015).

Instructions for participants:

The following instructions were given to participants before the interview:

- The purpose of the interview: “The interview aims to gain insights into your perception of online privacy and security risks in business.”
- Duration: “The interview will take about 30 to 45 minutes.”
- Volunteer participation: “Participation is voluntary and you can withdraw from the study at any time without any consequence.”
- Confidentiality: “All information provided will be kept confidential and anonymised in the final report. Your name and company are not linked to any responses.”

Preparation:

The participants were informed of the topics to be covered during the interview. This gave them time to think about their experience and prepare for discussions.

Data collection to understand online privacy and security perceptions

According to Creswell (2013:15), the data collection process is critical to producing information that helps answer research questions. As described in the previous section, qualitative research often relies heavily on interviews to obtain nuanced information about a phenomenon. To understand how businesses view online privacy and security in SMEs in CSA, interviews are seen as a valuable tool for obtaining more detailed insights. Such interviews allow for responses that cater to the nature of the subject matter (Bryman *et al.*, 2014:223). For this study, the researcher collected data primarily through interviews. Quinlan (2011:289) classifies interviews as follows:

- Online interviews.
- One-to-one interviews; and
- Telephone interviews.

Adopting these interview formats aims to have conversations with the participants while ensuring that the discussions remain focused on the research goals. Given the increasing importance of privacy and security, conducting one-on-one interviews at some of the entities was prioritised. During these interviews, selected owners and/or managers of SMEs in CSA participated in discussions. This approach allowed the researcher to investigate the business perceptions and online practices of SMEs (Quinlan, 2011:289). Specific interview questions can be found in the Appendix section.

Scheduling online interviews was suggested through platforms such as Zoom, Telephone or Microsoft Teams. To ensure that emails are not missed or marked as spam, custom subject lines and email content were created that emphasise the importance and relevance of the research to the recipient's industry or field of expertise. Furthermore, follow-up emails and reminders were sent with concise and persuasive overviews of research goals and potential advantages of participation. The use of contacts or referrals also increases the credibility of the invitation and increases the chances of a response. This method aims to provide ease and accessibility for participants, recognising that many supervisors may swiftly disregard emails. The option of conducting interviews online allows the participants to participate from their homes or workplaces, enhancing their opportunities. Bryman *et al.* (2015:227) highlight the advantages of this environment as it allows interviewees to feel more comfortable in a setting that fosters openness and comprehensive engagement.

At the beginning of each session, the researcher described the study objectives, expressed gratitude to the participants and asked for their consent to record and take notes. It is essential to employ recording equipment to ensure data collection and clarity (Smith, 2018). Ethical considerations are crucial throughout this process; the participants were reminded of their right to withdraw at any time while being assured of confidentiality. This assurance extends to protecting the anonymity of the participants and utilising the collected data to explore how SMEs in CSA view privacy and security (Bryman *et al.*, 2015:127).

In accordance with the POPI Act, all recorded interviews were kept secure and transcribed. These transcripts were treated as material accessible only to the researcher and authorised personnel involved in the study. Furthermore, data were stored on encrypted devices and password-protected servers to prevent access. According to the POPI Act regulations, recorded interviews and transcripts will be retained for five years (Department of Justice and Constitutional Development, 2013:818).

Qualitative analysis to examine factors that influence business perceptions of online privacy and security risk among SMEs in CSA

The researcher's goal is to explore how CSA businesses perceive risks related to online privacy and security, especially when engaging SMEs. To uncover these insights, a systematic approach was implemented to collect and analyse the data.

1. Data collection

- 15 semi-structured interviews with managers and owners of SMEs were conducted to gain an idea of their views on privacy and security.
- 15 semi-structured interviews were carefully recorded using voice recorders to ensure a reliable set of data (Smith & Lang, 2016:122). The participants were informed of the recording process and obtained written consent before recording (Smith & Lange, 2016:122).

2. Transcription and coding

- All the recorded interviews were transcribed and converted to a printed format for analysis.
- Taking cues from Bryman *et al.* (2014:336), the initial data were subjected to coding procedures. This involves transforming the data into a structure that can be easily understood by the researcher, allowing the extraction of insights.

3. Thematic analysis

A thematic analysis was performed to uncover patterns, themes and underlying meanings to go into the data gathered from the interviews. It is crucial to emphasise that the identification of themes occurred after an in-depth analysis of the interviews. This method allows for investigating how individuals view and experience online privacy and security in SMEs in the CSA region. The study included categorising the data to uncover themes and trends (Braun & Clarke, 2006). Themes were surfaced through a step-by-step

process involving immersing in the data, getting familiar with it, categorising and developing themes. Using this method, the study aims to provide information on the factors that shape business opinions and the practices of SMEs regarding privacy and security.

- Considering the nature of the study, Braun and Clarke approach is essential. According to Braun and Clarke (2006:87), this method involves immersing oneself in the data, creating codes that identify themes, refining them and ultimately producing a scholarly report.
- Thematic analysis strictly adhered to the phases outlined by Clarke (2006:87): familiarisation with the data, generating initial codes, searching for themes, reviewing themes, defining and naming themes and producing the report.

Online privacy and security: Trustworthiness in examining business perceptions

When it comes to privacy and security for CSA SMEs, it is crucial to ensure that the research is trustworthy. The reliability and validity of the term have traditionally been used in research. Qualitative researchers have also begun to use these terms to indicate the rigour, quality and greater applicability achieved by adhering to methodological standards (Bryman *et al.*, 2014:43). In this study on the factors influencing business managers' perceptions of online privacy and security risks, the researcher will assess both validity and reliability. Validity, in this context, refers to how research captures the truth about SME managers' views on privacy risks (Creswell & Creswell, 2018:199). On the other hand, reliability addresses the consistency of the results if other researchers replicate such a study.

To evaluate the validity of this study, a review technique was used that allowed the participants to reflect on the summarised findings of their perceptions. The goal is to determine whether your interpretations align with your thoughts about privacy and security risks. The interview guide was designed to frame the questions in a way that does not lead the participants towards specific answers.

According to Bryman *et al.* (2015:4445), trustworthiness can be understood through four pillars.

- *Credibility*: SMEs were allowed to confirm or adjust their understanding of privacy perceptions. Any new insights or suggestions the researcher provides will be considered, validating the respondents' views (Bryman *et al.*, 2015:44).
- *Transferability*: Considering the paced changes in privacy trends, ensuring that the findings can be applied to various situations is crucial. The researcher presented a detailed analysis of the results to enhance the study's transferability. This allowed the reader to compare the scenarios with the context of the study. The goal was to achieve understanding by conducting six interviews, thus achieving saturation.
- *Dependability*: The entire research process, from interviewing subject matter experts to analysing the data will be thoroughly documented to ensure a traceable methodology. By adopting a well-documented approach, the researcher can improve the study's credibility and facilitate audits (Bryman *et al.*, 2014:45).
- *Confirmability*: To ensure that the results accurately represent the information collected without prejudice that influences the findings, the researcher consulted with both the study supervisor and an expert in research. When credibility, transferability and dependability are achieved, it naturally results in confirmability (Bryman *et al.*, 2014:45).

In summary, it is crucial to consider the importance of trustworthiness when exploring perceptions regarding online privacy and security among SMEs in CSA.

1.9 ETHICAL CONSIDERATIONS

Before conducting the interviews, the researcher obtained consent from all the participants. This ensured that they fully understand the research objectives and their rights as participants. The study strictly adhered to the confidentiality and anonymity guidelines, guaranteeing that no identifiable information was disclosed in the final report.

1.10 ETHICAL PROTOCOLS

INFORMED CONSENT

Before the interviews were conducted, participants were given a full information sheet outlining the study's procedures, objectives and rights. Each participant was asked to sign

a consent form affirming their voluntary participation and comprehension of the study. They were informed that they may withdraw at any given time without consequence. Prior to beginning data collection, written and digital consent were sought. Informed consent ensures that participants understand the research's objective and implications before choosing to participate (Saunders *et al.*, 2019; Babbie, 2020).

ANONYMITY

Throughout the study process, participants' identities were kept confidential. No names, company identifiers or contact information were collected. Each participant received a unique code (e.g., P1, P2) to substitute their name in transcripts and analyses. Direct quotes utilized in the study were rigorously filtered to remove any identifiable information. Protecting participants' anonymity builds confidence and promotes honest participation (Creswell & Creswell, 2018).

CONFIDENTIALITY

Following the guidelines set out in the POPI Act, maintaining the safety and privacy of data is crucial. The collected information was strictly used for research purposes only, in compliance with the regulations outlined by POPIA. This is particularly important given the nature of decision-making and operations in SMEs on the popular online retail platform.

Data collections were carried out in compliance with the POPI Act. The participants were notified that their information would only be used for research purposes. They retain the option to withdraw at any point. Before their participation, explicit consent was sought from all the participants.

Confidentiality was preserved by ensuring that all obtained data were securely stored and only accessed by the researcher. Personal information and interview transcripts were password-protected and stored on encrypted devices. During reporting, no identifiable information was associated with any participant or SME. The POPI Act (Act No. 4 of 2013) requires all personal and corporate data to be gathered, stored and processed in a way that respects privacy and prevents illegal access (Republic of South Africa, 2013).

In addition, the information provided in the interviews is kept separate from those who provided it to protect their identities. This indicates that no reports, publications or presentations arising from this research will link any responses or opinions with people. Instead, generic names or pseudonyms shall represent them, ensuring that their anonymity is maintained. The applicable rules and institutional policies on data protection and preservation govern all data storage. Typically, such protocols outline the period during which information should be retained after the investigation. Therefore, the identified records are kept in safe custody for a specified period according to the organisational policy or relevant regulatory requirements. When this duration lapses, all data will be deleted from storage media or destroyed to comply with privacy laws and ethical norms (Saunders *et al.*, 2015).

DATA STORAGE AND DISPOSAL

Audio recordings, interview transcripts and consent forms were safely kept in password-protected folders. Physical documents were kept secured in a cupboard in the researcher's office safe. In accordance with the North-West University's data management policy, the data will be kept for five years following publication, after which all files will be permanently removed or destroyed. Data must be properly stored and responsibly discarded after the retention period in accordance with institutional and national privacy legislation (Resnik, 2020; POPIA, 2013).

ETHICAL COMPLIANCE

The North-West University Research Ethics Committee (NWU-01737-24-A4) approved the project. Ethical compliance safeguarded all participants' rights, dignity and safety throughout the research procedure.

CONCLUSION

The advent of the digital era has presented businesses, particularly SMEs, with incredible possibilities for growth. One key avenue to take advantage of these opportunities is to use online retail platforms such as local grocery stores and regional retail chains. By examining the insights shared by the managers of these online retail platforms, this study aimed to shed light on the potential benefits that SMEs can experience in this landscape, instilling a sense of optimism and hope. Growth in SMEs contributed to South Africa's

total GDP growth from only 18% in 2010 to 40% in 2020, demonstrating its significance to the country's economic landscape (Finmark Trust, 2020). At the same time, the qualitative discoveries show that although online retail platforms give them wider reach, it is not without difficulties, including managing digital procedures, handling virtual trading situations and maintaining a steady product standard.

The report emphasised that the gap between legally recognised companies and informal companies in SA, particularly with the introduction of COVID-19 relief measures, has presented a challenge to entrepreneurs. This is especially difficult because most (58%) of the companies operate without a legal organisation, which requires a delicate balance of embracing different companies while meeting the regulations in place. (FinMark Trust, 2020). Given their difficulties, SMEs' strength and versatility on digital platforms are impressive. They have used the advantages of such platforms to invent new ideas and adapt to changing markets. The heads of the online platform must prioritise creating beneficial conditions for SMEs. This includes offering resourceful assistance and workshops and making laws and regulations practical to address their needs and challenges. Furthermore, a complete connection with small businesses could trigger a full understanding of their concerns, resulting in more thoughtful and powerful plans. The outlook for small and medium companies in South Africa's digital marketplace is optimistic. Given the proper assistance of online platforms, managers and a supportive government policy, unlimited opportunities arise for expansion and creativity.

1.11 CHAPTER SUMMARY

The booming development of online platforms has significantly altered how businesses and SME managers interact. Although there are many potential benefits, there have been concerns about privacy and security in the areas of CSA. As a result, this study will use a qualitative approach to analyse managerial insights on online privacy and security threats in the region, considering its effects on the opinions of SME managers.

Context

Digital activity has increased in CSA due to the online presence of online retail platforms such as local grocery stores and regional retail chains, responding to the ever-increasing

demand from SME managers. This has also posed the need to prioritise and focus on online security and privacy (Smith, 2019b:45).

Objectives

To gain insights into how online platform managers from CSA formulate their views on business perceptions of online privacy and safety risks.

Methodology

Interviews were conducted with crucial website managers based in CSA. They were given a semi-structured form of questioning to express their perspectives while addressing the primary queries. Later, the data were interpreted through a theme identification process to identify issues relating to SME managers' opinions (Braun & Clarke, 2006:83).

Key findings

Trustworthiness of online platforms: Platforms with established reputations have SME managers who are more likely to trust their privacy and security protocols, which is essential for their credibility and reputation (Johnson, 2020: n.p.).

Transparency and communication: Managers of SMEs have a more favourable opinion of online platforms that actively explain their data protection and security policies (Davies, 2021: n.p.).

Past experiences: The increasing prevalence of data breaches and cyberattacks on popular platforms has exacerbated negative attitudes towards online security and privacy, leading to a decline in trust in such services.

Regulatory framework: A well-regulated environment strengthens the trust of SME managers by providing safeguards for their data, whereas weak or inadequate regulations lead to mistrust and scepticism. Walker (2018) emphasises the importance of robust regulations in protecting managers' data and promoting their confidence.

Implications

This research highlights the importance of online platforms in CSA to prioritise transparency, invest in security infrastructure and build trust with their SME managers.

Additionally, regulatory bodies must implement strict procedures to ensure the data protection of SMEs and create a secure online environment for managers.

Importance of the study

This study provides important information for those managing online platforms, policymakers and researchers in the field of online security and privacy. It emphasises that SME managers' perceptions of online security and privacy are multidimensional and that a comprehensive approach is necessary to enhance online security and privacy in CSA effectively.

1.12 THE LAYOUT OF THE STUDY

This academic study is structured into four chapters.

Chapter 1: Nature and the scope of the study

The study started by describing the topic under investigation. It clearly stated the problem being addressed, along with its objectives and the methodology used for research purposes. It also acknowledged any limitations present in the study.

Chapter 2: Literature Review

It covered the research and theoretical foundations to investigate the aspects that impact how businesses perceive privacy and security risks in SMEs in central South Africa. It delved into the literature on cybersecurity procedures, online privacy issues and regulations such as POPIA and the General Data Protection Regulation (GDPR). The section also highlighted areas where further research is needed, specifically in the South African setting, and laid the groundwork for comprehending how SME handle these risks.

Chapter 3: Empirical study

Chapter 3 discussed the study's findings, during which the researcher carefully examined the data and conclusions drawn from the study.

Chapter 4: Conclusion and recommendations

The research results were used to conclude the issue under investigation. The discussion considered whether the objectives were achieved and proposed research based on empirical evidence and the literature review.

1.13 Conclusion

To summarise the discussion, this study has established the basic structure for examining the elements that impact how businesses view privacy and security risks among SME in central South Africa. This section has presented the issue being researched and stressed the importance of comprehending how these companies manage the obstacles related to online privacy and security in a rapidly evolving digital landscape. The study aimed to explore how small businesses view and handle privacy and security risks and analyse how these views impact their day-to-day operations. The section highlighted the significance of this research in adding to the conversation on trust and security in central South Africa's economic and geographic setting.

The study's purpose was established by highlighting the gaps in the literature and discussing their significance for business leaders and policymakers involved in digital business activities. The introduction outlined the research direction clearly and paved the way for an in-depth review of existing literature, followed by empirical research. Chapter 1 sets the stage for the rest of the chapters by outlining the study's scope and importance, which will be further explored in the sections.

1.14 Chapter Summary

Chapter 1 delved into the core research focus on how different factors impact businesses' perceptions of privacy and security risks in SMEs in central South Africa. It laid out the objectives of the study, which involve grasping the obstacles businesses encounter regarding privacy concerns and their effects on business activities, as well as how enterprise's view and handle security risks. The first chapter paved the way for an examination by explaining concepts, the study's relevance and the research scope.

The study clearly outlined the research issue by underscoring the escalating significance of privacy and security in today's era. In the chapter's content, the necessity for this research was emphasised by exploring the growing dependence on channels and the subsequent surge in worries concerning data safeguards and security. It also examined

the queries steering the study. They validated why SMEs in central South Africa were chosen as the focal point, highlighting their pivotal economic role in the region and their distinct obstacles compared to more prominent companies.

Chapter 1 solidified the framework. It demonstrated how the study aligns with previous research materials while establishing the groundwork for a more in-depth examination in the following chapters

CHAPTER 2: LITERATURE REVIEW

2.1 INTRODUCTION

The rapid progress of technology and the growing reliance on internet platforms have brought about notable changes in the business landscape. This shift has introduced a range of possibilities and challenges to businesses worldwide; and the key concerns include privacy and security risks with a particular focus on SMEs in central South Africa (CSA) (Van der Merwe, Van der Walt & Van Rensburg, 2019:45; Hinson & Boateng, 2020:75). With the increasing digital interactions between companies and their stakeholders comes a growing concern about data breaches and cyber threats (Ilyoo & Hoon, 2013:929). It is crucial to grasp the factors influencing how businesses view privacy and security risks in the context of SMEs operating in regions like Bloemfontein, Potchefstroom, Sasolburg, Parys and Klerksdorp in CSA.

This literature review examines the current understanding of how businesses perceive online privacy and security risks. This chapter analyses theoretical frameworks and real-world examples to uncover meaningful patterns and areas where the existing research may be lacking. In addition to that overview, the research project will lay the groundwork for exploring the factors influencing how SMEs engaged in CSA, perceive and react to online privacy and security risks. Grasping these viewpoints is essential as they can impact how enterprises decide on and allocate resources for cybersecurity initiatives. It also affects their adherence to regulatory standards and helps them stay ahead in a competitive digital market (Arora *et al.*, 2021:120).

This part of the chapter delves into frameworks that form the basis for comprehending how enterprises view online privacy and security risks. The Unified Theory of Acceptance and Use of Technology (UTAUT2) (Venkatesh *et al.*, 2012:157) presents a thorough perspective on how enterprises adopt and implement technology. UTAUT Version 1 examines ideas, like performance expectations and ease of use to analyse how social factors and environmental conditions impact how businesses view security risks when implementing technology. In addition, the Cybersecurity Risk Management Framework (CRMF) (NIST, 2018:21) offers a method for enterprises to recognize, evaluate and reduce cybersecurity risks online. In today's world, this new system

empowers enterprises to establish a structured approach for addressing privacy issues and cybersecurity risks in the era of digitisation.

Additionally, according to the Diffusion of Innovation Theory (DOI) (Rogers, 2003:221), businesses still need to understand how they incorporate technologies to enhance their cybersecurity measures. The emphasis lies on the commonly perceived benefits and the seamless incorporation that motivates the implementation of security protocols. Modern frameworks offer a foundation for studying how SMEs in CSA view and address online privacy and security risks.

The literature review then delves into empirical studies investigating how businesses view the risks associated with privacy and security, concentrating on studies carried out worldwide and in local settings. This part focuses on the elements that impact these perspectives, including the size of the organisation, industry sector, past encounters with cyber events and understanding of regulations (Smith *et al.*, 2020:333; Hinson & Boateng, 2020:78). Research indicates that smaller businesses including SMEs frequently struggle with limited resources and expertise when it comes to establishing robust cybersecurity protocols. The online platforms' lack of clear communication and transparency can intensify businesses' concerns about vulnerability and potential risks (Jones *et al.*, 2019:105). In the realm of CSA, businesses face added complexity in navigating requirements. Compliance with laws like the Protection of Personal Information Act (POPIA) and global standards such as the General Data Protection Regulation (GDPR) is essential for businesses to safeguard online privacy and ensure data security. This intricate landscape shapes how companies approach and handle these risks (Van der Merwe *et al.*, 2019:48; Louw, 2020:64).

Furthermore, the chapter examines the literature on how businesses view privacy and security risks and how these affect their operational decisions, such as adopting technology upgrades, investing in cybersecurity measures and customer relationship management (CRM). According to Lee and Hong (2022:145), companies that view risks as significant were inclined to allocate resources towards enhancing their cybersecurity measures and providing training programmes for their employees, whereas organisations perceiving levels of risk might postpone or reduce investments in such initiatives. In this part of the discussion, we also examine variations in how

risks were viewed across different regions. This variation is shaped by elements such as the state of infrastructure, regulatory compliance levels and socioeconomic circumstances (Maree, 2019:55).

The literature selected for this review was chosen based on criteria to ensure coverage and relevance. Although the primary focus was to analyse research papers from 5 to 10 years ago to capture current trends and developments, foundational studies play a crucial role in grasping essential theoretical frameworks. Seminal works by Davis (1989:320), Rogers (1975:93) and Ajzen (1991:179), while they were written years ago, are still relevant today in shaping research frameworks like the Technology Acceptance Model (TAM). These early works continue to play a significant role in contemporary academic discussions by providing a robust theoretical groundwork, for understanding how businesses view and address the challenges of online privacy and security.

The review includes articles from journals that have been reviewed by peers, as well as books and reliable sources sourced from academic databases like JSTOR. Scopus and Google Scholar were also used to gather information. Additionally, CSA and other developing regions were particularly emphasised in comparing their views of the enterprise and meaningfully addressing privacy and security risks (Kareem & Johnson, 2021:112). This strategy application in the chapter content evaluation scrutinises previous studies, emphasises areas lacking research and stresses the necessity for additional exploration in this field. The results of this analysis will guide the development of research plans and methodology and help shed light on how SME in CSA handle the intricate realm of online privacy and security.

2.2 THEORETICAL FRAMEWORK

The researcher used a theoretical framework to analyse the key concepts and relationships that impact online privacy and security risks. This structured approach helps them to understand the factors influencing their business perceptions. This research builds on established theories that have played a key role in understanding the concepts of online privacy and security perceptions and behaviours in business settings. Some theories mentioned are the TAM, the TPD and the protection motivation theory (PMG).

2.2.1 Technology Acceptance Model (TAM)

Davis (1989:319) introduced the TAM, a framework used to explore the process of individuals and organisations embracing novel technologies. Based on TAM insights, the main drivers that affect technology adoption are its ease of use and perceived helpfulness. In the realm of privacy and security concerns, TAM has been used to explore business attitudes towards and acceptance of security technologies (Aloul, 2019:48). Businesses might consider how easy it is to integrate a cybersecurity solution and if it helps lower their concerns about data breaches or other online risks (Venkatesh & Davis, 2000:189).

Research findings have expanded the TAM to incorporate other factors important in online security, such as trust and risk perceptions (Pavlou, 2020:125). How security technologies and vendors are perceived in terms of trustworthiness and the risks associated with using or not using these technologies can significantly impact how businesses make decisions (Gefen *et al.*, 2018:409). In the context of this study, it is essential because it explains how companies in the cybersecurity industry make decisions about investing in security tools based on their perceived usefulness and ease of use, while considering their trust in technology providers and their awareness of online security risks.

2.2.2 Theory of Planned Behaviour (TPB)

The TPB introduced by Ajzen (1991:180) offers a perspective on how businesses approach online privacy and security concerns in decision-making. TPB proposes that a person's actions are shaped by their desire to carry out those actions; this desire is further affected by their beliefs, personal norms and perceived ability to act. This concept has been widely used in research exploring how organisations behave when implementing privacy protocols and security measures (Yoon, 2019:74). In the realm of SME experiences, TPB sheds light on how the views held by business proprietors or managers on online security and their belief in social expectations or standards regarding security procedures influence their choices to adopt privacy and security measures based on their confidence in executing such measures effectively (Bulgurcu *et al.*, 2010:525). For example, when business owners see the importance of having cybersecurity precautions and sense social expectations from clients or partners, as

well as regulatory authorities push for it, they tend to embrace these safeguards more readily (Johnston & Warkentin, 2021:92). TPD provides a perspective on the mental processes involved in making decisions related to privacy and security in SMEs.

2.2.3 Protection Motivation Theory (PMT)

The Protection Motivation Theory (PMT) was first created by Rogers (1975:98); understanding how individuals react to dangers and risks is crucial when addressing issues such as online security threats. They also factor in the effectiveness of a protective action (response efficacy), as well as their confidence in executing that action (self-efficacy) (Rogers, 1983:155).

Researchers have used PMTs to investigate how companies evaluate and address cybersecurity risks (Boss *et al.*, 2020:289; Lee & Hong, 2022:143). Businesses often rely on this concept to assess the impact of cybersecurity threats and determine their investment in measures. If medical examiners feel there is a chance of data breaches and trust that cybersecurity steps can reduce these risks effectively, they are inclined to allocate resources towards implementing such measures (Johnston *et al.*, 2021:216). The research delves into how perceptions of risks and motivations impact business choices regarding privacy and security in the context of CSA using the PMT framework.

2.2.4 Relevance to the current study

These theoretical frameworks play a role in the study by providing different points of view on the factors that impact how SMEs perceive online privacy and security risks in the CSA region. TAM offered insights into how businesses view technology's ease of use and usefulness and its impact on adoption practices. This is especially significant in the context of cybersecurity technology implementation in organisations. The TPB provides insights into how attitudes and perceptions of control influence the decision-making process in businesses concerning security measures. Ultimately, PMT explains the motivational aspects that lead companies to implement security measures in response to potential online threats. This study combines different theoretical viewpoints to gain insights into what influences how SMES in the cybersecurity sector perceive online privacy and security risks in CSA. This knowledge

can benefit academic research and help develop effective strategies to improve cybersecurity resilience in this setting.

2.3 REVIEW OF CRITICAL THEMES AND TOPICS

The following section is a detailed overview of topics and themes shaping how CSA SMEs view online privacy and security risks. The evaluation is structured around five areas: (1) Risks associated with online privacy and security in business conditions, (2) Factors influencing how businesses view privacy and security risks, (3) The impacts of privacy and security risks on business functions, (4). Approaches utilised by firms to address online privacy and security risks, and (5) The influence of frameworks and how businesses perceive and handle online privacy and security matters.

2.3.1 Risks associated with online privacy and security in business conditions

Privacy and the risks related to security have become increasingly prominent in the past few years. This is mainly attributed to the shift towards digitalising business operations and the growing dependence on internet-connected technologies (Safa *et al.*, 2016:410). Online privacy risks typically refer to the dangers that personal or organisational information may face when collected, stored, transmitted and used online (Bansal *et al.*, 2016:980). On the other hand, security concerns involve risks and weaknesses that can endanger the secrecy and reliability of information and digital resources (Abawajy, 2014:116).

For SMEs, these risks are especially pronounced because they have fewer resources and less advanced cybersecurity systems than larger companies (Chen, 2019:67). Studies in the past have revealed a growing trend in which micro-enterprises are becoming prime targets for cybercriminal activities. SMEs frequently face heightened security risks due to security measures and a lack of awareness about cybersecurity among company leaders and managers. (Verizon, 2020:12). South Africa's online privacy and security challenges have become more complex due to the socioeconomic setting and regulatory framework. Complying with data privacy regulations and protecting information in businesses are aspects of enforcing the POPIA (Jones, 2022:218).

2.3.2 Factors influencing how businesses view privacy and security risks

It is essential to comprehend the aspects that affect how businesses view privacy and security risks to recognise obstacles to implementing effective security measures properly. According to studies on this topic, organisational culture awareness, perceived seriousness, susceptibility to data breaches and confidence in third-party suppliers all play a crucial role in shaping these perceptions (Li *et al.*, 2018:134). Numerous research papers emphasise how culture and knowledge influence people's views on online privacy and security risks (Aurigemma & Mattson, 2019:381). Organisations that value the cybersecurity culture tend to view privacy risks as necessary and actively work to address them. Businesses that are well-informed about cybersecurity risks tend to understand the importance of implementing security measures (Tsai *et al.*, 2017:610). In CSA SMEs, awareness and education on online privacy and security are often limited, making it challenging to adopt appropriate protective measures (Scholtz *et al.*, 2020:89).

2.3.3 The impacts of privacy and security risks on business functions

Privacy and security risks can have significant effects on business operations. Research has revealed that occurrences like data breaches and cyberattacks could result in financial losses and reputational harm for companies while also leading to buyers losing trust and potential legal issues (Romanosky, 2016:109). SMEs outcomes in such situations tend to be more severe as they struggle to cope with financial setbacks and repair their tarnished reputations (Gordon *et al.*, 2018:71). Research conducted in SA indicates that SMEs risk cyberattacks due to the rapid evolution of digital technology and the increasing expertise of cybercriminal actors (Mathews & Farnden, 2021:178). Furthermore, security breaches can have a lasting impact on SMEs beyond just financial losses, including diminished competitive edge and even the risk of shutting down the business in the long run (Miranda *et al.*, 2019:53).

2.3.4 Approaches utilised by businesses to address online privacy and security risks

Businesses worldwide have taken steps to safeguard their data and digital resources, considering growing concerns about privacy and security threats. Incorporating

cutting-edge cybersecurity tools and practices is crucial to preserving information. Educating staff about security measures and implementing data protection protocols are essential. Furthermore, collaborating with external security experts can further enhance protection (Siponen & Vance, 2018:92). SMEs professionals frequently need help implementing these plans because of resource limitations and a lack of access to know-how. They also need help recognising the solutions within reach (Tikkinen-Piri *et al.*, 2018:279). Recent research in CSA indicates that although specific SMEs are implementing fundamental security measures like firewalls and antivirus software systems, a significant number of them do not possess thorough policies for safeguarding data and offering security awareness training to their employees (Nkomo & Mashiane, 2020:104). Additionally, financial limitations and doubts about technology suppliers frequently impede the implementation of cutting-edge security technologies (Puhakainen & Siponen, 2017:118).

2.3.5 The influence of frameworks on how businesses perceive and handle online privacy and security matters

Regulations greatly influence how businesses view and approach privacy and security measures. In the legal system of SA, the POPIA, enacted in 2021, outlines rules regarding how personal information is collected, stored and handled (Maduku, 2021:232). This law has prompted businesses to review how they protect data and implement security measures to meet regulatory standards (Nkosi, 2022:134). Research has shown that adhering to regulations can significantly improve cybersecurity measures. Many companies see compliance as an expense rather than a valuable investment, especially SMEs (Dlamini *et al.*, 2019:142). Among SMEs, compliance challenges often arise due to a lack of understanding and awareness regarding regulatory requirements in CSA (Singh & Van Belle, 2020:94). Furthermore, frameworks alone may not be enough to encourage companies to implement comprehensive data protection measures unless they are supported by awareness campaigns and assistance programmes (Ramokgadi & Katuu, 2021:77).

2.3.6 Gaps in the literature

Although researchers have extensively studied privacy and security risks, unresolved gaps and inconsistencies in the existing literature requires attention. Most of the

research conducted so far has primarily focused on large corporations and has tended to draw broad conclusions that apply to all kinds of businesses. This approach has resulted in a lack of information on SMEs' unique obstacles and perspectives, especially in various regions, such as SA (Bisson, 2019:214). Furthermore, research has delved into how cybersecurity awareness and company culture influence people's views on privacy. However, there has not been an empirical study of how these factors interact with the regulatory and socioeconomic conditions of CSA specifically (Scholtz *et al.*, 2020:90). There has not been research on how SMEs in CSA view and apply the rules of the POPIA, even though it was recently introduced (Maduku, 2021:234).

There is also a lack of research regarding how trust in third-party vendors influences the adoption of cybersecurity practices among SMEs. Many modern organisations heavily depend on third-party vendors' IT and cybersecurity services. This aspect presents an area for future investigation (Aurigemma & Mattson, 2019:382). Long-term studies are required to understand the evolution of business attitudes towards privacy and security risks over time. For businesses to safeguard privacy and security effectively, they must stay vigilant against threats and adapt to changes in regulations that impact their operations significantly (Romanosky, 2016:111).

2.4 CRITICAL ANALYSIS OF REVIEWED LITERATURE

When examining the research on online privacy and security risk in CSA for SMEs, it is essential to assess the strengths and weaknesses of the reviewed studies, as well as their methods and conclusions. In this part of the discussion, the researcher explores the strengths and limitations of research work and how my study aims to expand on or question these established findings.

2.4.1 Strength of the existing literature

Numerous research papers offer valuable perspectives on the risks associated with online privacy and security in business environments, explicitly emphasising awareness levels, organisational culture dynamics and the impact of regulatory frameworks. A model, Safa *et al.* (2016:410) created for information security policy compliance has been extensively referenced and applied to comprehend the factors affecting organisational compliance behaviour. The use of techniques to confirm the accuracy of their model and the wide range of data they collected from various sectors

strengthens the validity of their conclusions. Likewise, the research conducted by Tikkinen-Piri *et al.* (2018:137) delineates the impact of the European Union's GDPR, shedding light on its repercussions for businesses. This research examines a significant change in regulations and how they influence business operations. Dlamini *et al.* (2019:142) examine the landscape in SA, focusing on the impact of the POPIA on businesses' information security protocols. They adopt a case study method to explore the hurdles and adjustments faced in this context.

2.4.2 Limitations of existing literature

While these positive aspects are commendable, the literature also exhibits some drawbacks. According to Safa *et al.* (2016:410) and Tikkinen-Piri *et al.* (2018:136), numerous research projects mainly concentrate on companies or fail to make distinctions among various kinds and scales of companies. Their discoveries may not be as relevant for SMEs, as these entities might possess varying resources and levels of awareness and susceptibility. Additionally, the research conducted by Dlamini *et al.* (2019:141) is mainly focused on descriptions without delving into the underlying factors that drive businesses to adopt or shun practices, which is a crucial aspect unaddressed in their study methodology despite providing detailed insights based on case studies; however, its applicability to a broader audience may be limited due to this constraint.

Many studies also face challenges in their methodology. For example, Li *et al.* (2018:137) provide valuable insights into consumer privacy behaviours. However, their research mainly uses self-reported data, which can lead to biases such as social need or memory biases. In addition, according to Noksi (2022:135), adherence to POPIA regulations mostly depends on survey information that can be beneficial in identifying patterns but may not delve deeply into cybersecurity challenges specific to SMEs.

2.4.3 Areas where the literature is robust

The current body of research is quite comprehensive, including topics such as the influence of privacy and security risks on businesses, the regulations that influence business operations and the joint cybersecurity approaches that companies adopt. Romanosky (2016), for example, evaluates the expenses and origins of cyber

incidents, providing valuable insights that can guide decision-makers in the government and corporate sectors. The results from research, such as the study conducted by Miranda *et al.* (2019) about advancements in SMEs, offer valuable perspectives regarding how businesses address issues related to online privacy and security in a tailored manner. Exploring the impact of culture and awareness on cybersecurity perceptions and practices is a robust area in the literature (Aurigemma & Mattson, 2019:381). These research efforts hold importance in uncovering the elements that shape how businesses address cybersecurity challenges and lay the groundwork for future exploration in this field.

2.4.4 Areas where the literature is lacking

However, the research is lacking, especially regarding SMEs in some geographic regions, such as CSA. Many research studies make assumptions about businesses in general without considering the specific obstacles and resources that microenterprises face (Bisson, 2019:210). SME employees may not have access to in-depth studies on how they view privacy and security risks, given their limited resources and less advanced security systems. Furthermore, many research studies examine the effects of guidelines such as POPIA. However, there is a lack of data regarding how SMEs in SA implement these regulations (Maduku, 2021:232). The current body of work also does not include studies that follow how business' views and behaviours change over time in response to regulatory changes and challenges. Conducting research is crucial to understanding the ever-changing landscape of cybersecurity risks and helping businesses adjust appropriately (Romanosky, 2016). Moreover, there is a lack of investigation into how trust in third-party suppliers influences cybersecurity procedures in SMEs. This oversight is essential since numerous medical examiners depend on companies for IT and cybersecurity requirements (Aurigemma & Mattson, 2019:400).

2.4.5 How will the research build upon or challenge the existing literature

My study seeks to expand and question the body of knowledge in various ways. It will primarily focus on SMEs in CSA, filling the void in geographical and contextual details. This study aims to offer in-depth qualitative perspectives into the obstacles that SMEs encounter in this area by using formal online discussions with entrepreneurs and supervisors in the field. Issues are frequently ignored in more general research

studies. To sum up, this research will examine how SMEs navigate factors of cultural awareness and compliance with POPIA. It will also investigate the regulatory landscape of SA, explore how SMEs interpret and put into practice data protection regulations and shed light on the various factors that impact compliance with these rules. Given the scarcity of evidence, it is worth noting how businesses in SA handle the intricacies of regulatory structures such as POPIA.

Additionally, this study will explore the importance of trust in third-party suppliers and its impact on SMEs implementation of cybersecurity measures. This area has not been extensively researched in the existing literature; however, it is essential to grasp the range of obstacles and potentials that SMEs encounter to improve their cybersecurity defences. Finally, this research will investigate the real-life experiences of business owners and managers as they navigate the challenges of privacy and security risks using a qualitative research methodology. This method aims to enhance understanding by offering a more nuanced perspective on how SMEs view and handle online privacy and security risks compared to traditional quantitative studies.

The current body of work on the risks associated with privacy and security risk provides valuable perspectives on different facets of this subject matter; however, it is not without its shortcomings, particularly in the case of SMEs operating in specific settings such as those found in CSA. This study aims to address these gaps through research by examining SMEs in CSA, delving into adherence and the importance of trust in third-party suppliers and considering the real-life experiences of business owners and managers. Using this method in this research project, the researcher aims to add depth to the knowledge about the dangers of online privacy and security. The findings will guide policymakers, corporate executives and scholars alike.

2.5 CONCLUSIONS

The literature review focuses on how SMEs perceive the risks of online privacy and security in the context of CSA relationships. Online privacy and security risks are thought about along with how businesses view them and their effects on their operations, the strategies they use to manage these risks and how regulatory frameworks influence business practices. The results highlight the need to understand these elements to strengthen cybersecurity readiness among SMEs in CSA. The

literature review has pointed out some discoveries in examining online privacy and security risks for SMEs. Previous studies offer perspectives on how concerns about online privacy affect business operations in terms of organisational culture and regulatory structures. Research conducted by Safa *et al.* (2016) highlighted how adherence to rules and alertness can significantly boost cybersecurity measures. The work of Tikkinan *et al.* (2018) and that of the team led by Dlamini *et al.* (2019) shed light on the significant impact of regulatory standards such as GDPR and POPIA on influencing business operations. The literature strongly shows how organisational culture and compliance behaviour are closely related (Aurigemma & Mattson, 2019).

However, the evaluation also points out shortcomings and discrepancies in the existing pool of information. Numerous studies have focused on companies and broad conclusions have been drawn across all types of businesses without considering the distinct traits and difficulties encountered by SMEs, specifically in the context of CSA. There is a shortage of real-world data in the literature regarding how SMEs in SA handle and enforce data protection laws such as POPIA. Furthermore, there is a minimal investigation into how trust in third-party vendors impacts cybersecurity practices among SMEs. Furthermore, a significant issue is a lack of long-term studies to understand how businesses adapt their strategies and views in response to the evolving cybersecurity environment. This research seeks to fill these gaps by concentrating on SMEs in CSA and delving into their distinct struggles in handling online privacy and security risks. By exploring the importance of trust with external vendors, this study aims to improve understanding of how culture and awareness impact regulatory compliance in cybersecurity practices for SMEs.

In the next section of the report, the researcher will detail the approach taken to carry out the research for this study. The study will describe how the research was set up and conducted through formal online interviews with SME owners or managers and the methods used to analyse qualitative data using Braun and Clarke's (2006:87) approach to interpret the results. This structured method will guarantee that the research yields detailed and tailored understandings of the viewpoints and encounters of individuals in SMEs concerning privacy and security risks.

CHAPTER 3: EMPIRICAL STUDY

3.1 INTRODUCTION

This chapter provides a discussion of how the data were analysed. It presents the findings based on interviews conducted with owners and managers of small and medium-sized enterprises (SMEs) in the CSA region. The primary objective was to investigate the factors that influence how SMEs in CSA perceive, understand and manage online privacy and security risks. This was done with a particular focus on the e-commerce context, examining business perceptions, managerial knowledge, cultural and emotional influences and providing practical, context-specific recommendations to enhance security and privacy practices in the region. The themes revealed herein bear the underlying issues, values and coping mechanisms that inform managerial perceptions of cybersecurity in semi-urban economies. Not only are the practices of SMEs documented by this research, but the study also interrogates the motivations and justifications behind these practices.

3.2 Demographic characteristics of participants

The demographic profile of the study's participants reveals the heterogeneity of leadership among SMEs in CSA's semi-urban centres. Moreover, most participants possessed over a decade of experience in their respective fields. This was ideal for understanding the evolving nature of cyber threats. These enterprises were strategically located in key towns like Potchefstroom, Kroonstad, Kimberley and Bloemfontein. The extent to which SMEs utilised the online facilities varied depending on their levels of technical literacy and operational needs. However, it was noted that there was a reliance on internationally hosted cloud facilities, social media platforms and third-party systems, which was evident, thus raising issues about data sovereignty and foreign control. Moreover, the sample representation of SMEs across various sectors, including IT, retail, manufacturing, construction and consulting, encompassed a diverse set of sector-specific privacy and security concerns. This sampling composition substantiates contextualising awareness of cybersecurity among managers of SMEs in more profound structures of experience, digital infrastructure accessibility and locational dynamics.

Table 3.1. Demographic characteristics of the participants

Participant code	Role in business	Type of industry	Years of experience	Location in CSA	Online platform used
Participant A	Owner/Operator	Retail	5 years	Bloemfontein	Google Workspace, social media
Participant B	Director/Manager	Construction	20+ years	Sasolburg	WhatsApp, Cloud-based tools
Participant C	Founder	IT Solutions	10+ years	Parys	AWS, Facebook, Gmail
Participant D	Managing Director	Services/Retail	8 years	Kroonstad	Google, PayFast, Hosting SA
Participant E	Owner	Manufacturing (printing)	10+ years	Potchefstroom	WhatsApp, Google Suite
Participant F	IT Business Owner/Lead Developer	Software Development	10+ years	Klerksdorp	Google Cloud, GitHub
Participant G	Medium-sized enterprises Partner	Tech-related	7 years	Kimberley	Social media, Web Portals
Participant H	Developer/Director	Software Development	10 years	Potchefstroom	Google Cloud, Backups Monthly
Participant I	Owner/ founder	Logistics & distribution	12 years	Lichtenburg	Dropbox, WhatsApp Business, Zoho CRM
Participant J	Managing Director/CEO	Events Management	6 years	Bloemfontein	Instagram, Facebook, Website

Participant K	Founder	Events	4 years	Sasolburg	WhatsApp, Instagram
Participant L	Owner	IT Solutions	7 years	Kroonstad	WhatsApp, Instagram
Participant M	Owner/Manager	Retail	5 years	Bloemfontein	Social media

Source: Boqo, X. (2025). Researcher's own compilation from field interview data.

Table 3.2 below shows how the main themes and sub-themes align with the research objectives. The table also illustrates the connection between the specific aspects of participants' perceptions and practices regarding online privacy and security and the broader objectives of the research. Some of the themes generated include understanding the underlying influences, managerial knowledge, cultural and emotional factors, as well as opportunities for local innovation and policy guidance. The table provides a structured overview of the research's analytical framework.

Table 3.2. Alignment of themes with the research objectives

Theme	Sub-theme	Description	Alignment with the research objective
Underlying influences on business perceptions	<i>1.1 Cloud infrastructure dependency and risk trade-offs</i>	The themes indicate how reliance on global cloud platforms introduces both operational benefits, geopolitical and legal vulnerabilities.	Explore factors that influence business perceptions of online privacy and security risks.
	<i>1.2 Experiences of peers and risk narratives</i>	Reflects the role of informal peer learning and anecdotal evidence in influencing risk perceptions and security practices.	
Perceived risk in e-commerce and online business environments	<i>2.1 Privacy as a political and operational threat</i>	Concerns about foreign surveillance, legal access and the limitations of technical safeguards.	Explore how managers in SME view privacy and security concerns on online shopping sites in the CSA region.
	<i>2.2 Managing client trust on digital platforms</i>	Focuses on reputational risks, data minimisation and self-regulatory practices to maintain client trust.	
Leadership knowledge and	<i>3.1 Experience-driven cyber literacy</i>	Entails how managers build cyber literacy through trial and error, leading to practical, grassroots security routines.	Investigate the extent of comprehension and awareness

adaptive security practices			of privacy and security principles among the participants.
	<i>3.2 Legal awareness and responsibility</i>	Details the formalisation of data protection via NDAs, privacy briefings and onboarding.	
Cultural and political dimensions of cybersecurity	<i>4.1 Digital sovereignty as a national mandate</i>	Reflects concerns about foreign control of infrastructure and the drive for national autonomy in digital operations.	Examine the role of cultural & political contexts in shaping cybersecurity practices.
	<i>4.2 Ubuntu and technological solidarity</i>	Emphasises ubuntu as a guiding ethic for collective innovation, self-reliance and community-driven solutions.	
Emotional and psychological drivers	<i>5.1 Strategic fear and informed caution</i>	Reflects how fear of loss motivates vigilance and defensive routines in cybersecurity.	Investigate the emotional and psychological factors influencing engagement with cybersecurity.
	<i>5.2 Entrepreneurial optimism and agency</i>	Describes optimism and agency as drivers for proactive, innovative and adaptive security behaviours.	
Pathways for local innovation and policy guidance	<i>6.1 Collaborative pathways for local innovation</i>	Provides opportunities for local hosting, developer forums and open-source collaborations to build digital sovereignty.	Identifies opportunities for local innovation and the need for

			accessible, practical cybersecurity policy guidance.
	6.2 <i>Simplified, contextual policy guidance</i>	Highlights the need for concise, practical and visually accessible cybersecurity guidelines tailored for enterprises.	

Boqo, X. (2025). Researcher's own compilation from thematic analysis of field interview data.

3.3 Themes

The following section provides a discussion of the themes generated through thematic analysis. The primary objective was to explore how SMEs perceive and address digital privacy and security concerns in the context of the CSA's technological landscape. Each theme is supported by a visual figure that illustrates its sub-themes and interconnections, aiming to enhance conceptual clarity.

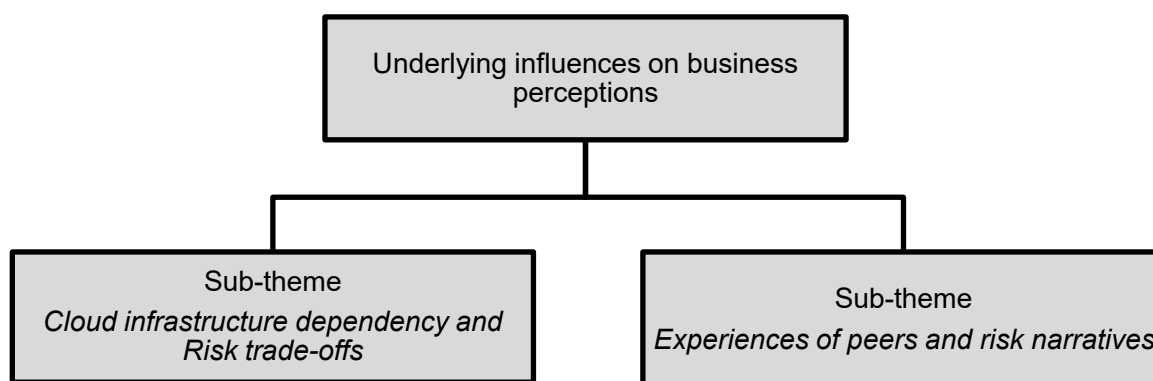


Figure 3. Themes generated from the research objective

Explore the factors that influence business perceptions

3.3.1 3.3.1 Theme 1: Underlying influences on business perceptions

The first theme is based on the underlying structural and experiential elements that could influence SMEs' perceptions of digital risk. The findings reveal that the perceptions of SMEs are not necessarily influenced by formal training or institutional guidance, but rather by peer influence and constraints related to cloud infrastructure. Figure 3.1 above visually captures this thematic structure. It illustrates how these underlying perceptions are influenced by other factors, such as reliance on external cloud services and informal methods of risk awareness through the experiences of their peers.

Sub-theme 1.1: Cloud infrastructure dependency and risk trade-offs

It appears there was consensus among the participants regarding the use and performance benefits of global cloud platforms such as Google Cloud, AWS and Azure. These services were praised for their reliability, scalability and user-

friendliness. However, there were also concerns regarding the legal and political risks associated with hosting data outside South Africa:

“We’re using the best platforms, but they’re not South African. We’re one political decision away from losing everything.” – Participant H

“Cloud tools make everything faster, but we constantly wonder what control we have.” - Participant B

“Hosting data overseas raises red flags. What if the laws there change or someone gains access without us knowing?” – Participant J

We can’t avoid global platforms, but it does make us think twice about where our data lives.” - Participant K

These quotations encapsulate what might be described as a state of *jurisdictional anxiety*, where SMEs recognise that their digital operational backbone lies outside their national regulatory framework. While technically efficient, this model of dependency introduces enterprises to geopolitical and legal risks that are essentially outside their control. This finding may suggest that the decisions of SMEs are not always technically or economically motivated. According to the participants, using cloud platforms such as Google Cloud, AWS and Azure can yield operational advantages. However, it can also expose SMEs to geopolitical challenges beyond their control. Li *et al.* (2018:134) also concur with this finding. They point out that the organisation's perceptions of privacy and security risks rely on factors such as trust in third-party providers and perceived susceptibility to data breaches.

Sub-theme 1.1 highlights how SMEs balance the trade-offs between utilising advanced cloud infrastructure and managing the legal and political vulnerabilities that arise from hosting data outside the South African jurisdiction. This state of jurisdictional anxiety reflects a broader cultural and experiential context in which SMEs operate. Aurigemma and Mattson (2019:381) argue that organisational culture and collective knowledge influence how businesses perceive and respond to online security and privacy risks. Due to a lack of formal cybersecurity training and institutional guidelines in CSA., risk awareness tends to be acquired informally through experiences of peers (Scholtz *et al.*, 2020:89)

This learning process then appears to influence perceptions and decision-making, typically complementing formal cybersecurity training. Tsai *et al.* (2017:610) also contribute evidence that enterprises with greater cybersecurity knowledge levels are more likely to recognise the necessity of instituting stringent security controls. However, reliance on foreign cloud service infrastructure, coupled with low domestic cybersecurity literacy, creates a two-sided context where SMEs must cope with both technical and geopolitical risks. The interaction between infrastructural dependencies and awareness of cybersecurity risks uniquely influences efforts to enhance resilience in the digital economy.

Sub-theme 1.2: Experiences of peers and risk narratives

Another key influence shaping perceptions of risk was informal learning through peers or local business networks. Rather than relying on formal cybersecurity training, SMEs often cited stories shared by their peers as the impetus for revising their data protection strategies:

“I heard from a friend how they lost client data when their hosting went down. That made me change my whole backup strategy.” – Participant F

“I’ve learned a lot from other businesses’ mistakes, hearing their stories shaped how cautious I became.” - Participant J

“When someone I know got hacked, it made me double-check all our settings the next day.” - Participant M

This sub-theme highlights the important role informal trust networks play in the dissemination of practical knowledge. While such informal learning can produce context-sensitive and responsive security practice, it may also be technically naive, with oversights or misleading advice being a risk for SMEs. However, it is an adaptive strategy that aligns with the resource constraints under which SMEs in the CSA typically operate.

3.3.2 Theme 2: Perceived risk in e-commerce and online business environments

As SMEs embrace digital commerce platforms to expand their market reach, they simultaneously encounter various vulnerabilities. Theme 2 discusses how digital expansion amplifies exposure to privacy threats and undermines managerial certainty, particularly in the absence of robust data governance mechanisms. Figure 3.2 illustrates the dual dimensions of this theme. The theme encompasses both political anxieties surrounding surveillance and legal access, as well as operational concerns related to maintaining client trust and protecting the enterprise's reputation.

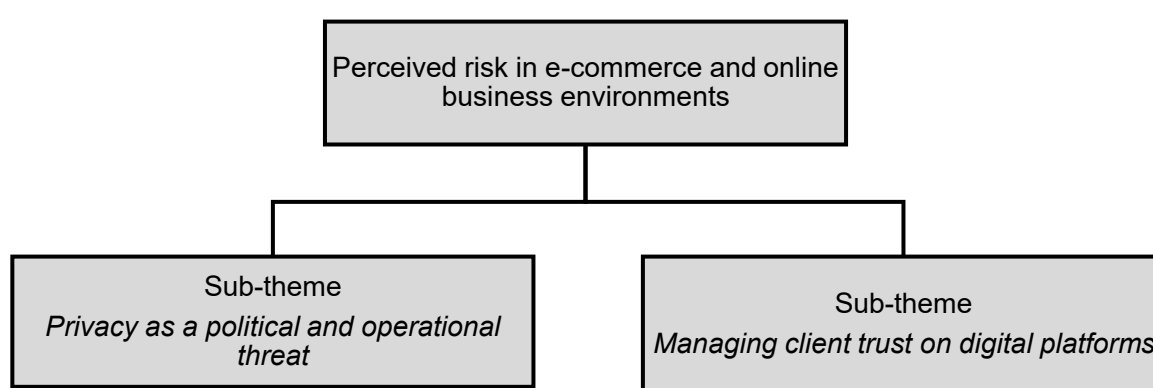


Figure 4. Themes that emerged from the research objective

Explore how managers in SMEs view privacy and security concerns on online shopping sites in the CSA region.

Sub-theme 2.1: Privacy as a political and operational threat

The participants expressed concerns regarding the level of encryption as a step that would protect information stored on foreign servers. Apart from the technical aspects, they were worried about the political environment in which such platforms operate, i.e., the ability of foreign governments to compel access to information.

“Even if platforms encrypt our data, who’s to say their governments won’t just demand access anyway?” – Participant C

This perspective advocates for a broader interpretation of privacy as a geopolitical threat, where data security is not just an issue of passwords and firewalls. It also

entails jurisdictional control and democratic accountability. SMEs appear intensely cognizant that using internationally hosted services subjects them to regulatory regimes over which they have no control.

Sub-theme 2.2: Managing client trust on digital platforms

The participants also discussed the reputational risks involved in handling client data. Several SMEs had adopted data minimisation measures, requesting only the necessary information to limit exposure in the event of a breach:

“We collect only what we need. A data breach could mean losing business forever.” – Participant A

“Our clients expect us to protect their information; it’s about trust, not just compliance.” – Participant D

“Even if the tech is secure, if clients don’t feel safe, we lose credibility.” - Participant H

“We avoid sharing too much online; we’d rather clients know we take confidentiality seriously.” – Participant C

Here, privacy is not only a regulatory requirement but also an ethical and reputational one. The participants noted that beyond meeting regulatory requirements, client data privacy is essential to maintaining trust and protecting the enterprise’s reputation in an increasingly competitive digital market. This perception is supported by Verizon (2020), which highlights the severe reputational risk that SMEs face due to data breaches. According to Verizon (2020), larger enterprises experience more severe consequences due to their reliance on close client relationships.

Even in the absence of robust local enforcement mechanisms, an emergent self-regulation ethos is in place, driven by the recognition that maintaining client confidence is essential for long-term survival. SMEs are proactively adopting data minimisation strategies. They are collecting critical information only to reduce their exposure and this demonstrates ethical stewardship of personal data. This self-regulation is evidence of strategic planning for both operational business risks and political operational risks in data governance. This is critical, particularly for platforms based

abroad that lack complete jurisdictional control (Jones, 2022:218). Thus, privacy management in such enterprises transcends technical controls. It is a holistic approach that encompasses ethical responsibility, reputation preservation and responsive governance. This shift in mindset reflects how SMEs are navigating the complex overlap between political, legal and operational challenges in protecting their customers and brands in the digital marketplace.

3.3.3 Theme 3: Leadership knowledge and adaptive security practices

Theme 3 provides a more in-depth discussion of the internal learning processes and adaptive behaviours exhibited by the leaders of SMEs. Lacking formal institutional support or training in cybersecurity, the participants demonstrated considerable initiative in developing their own protective routines and governance frameworks. As illustrated in Figure 3.3, this theme encompasses two closely related dimensions: cyber literacy gained through practical experience and the emergence of legal and procedural accountability in business operations.

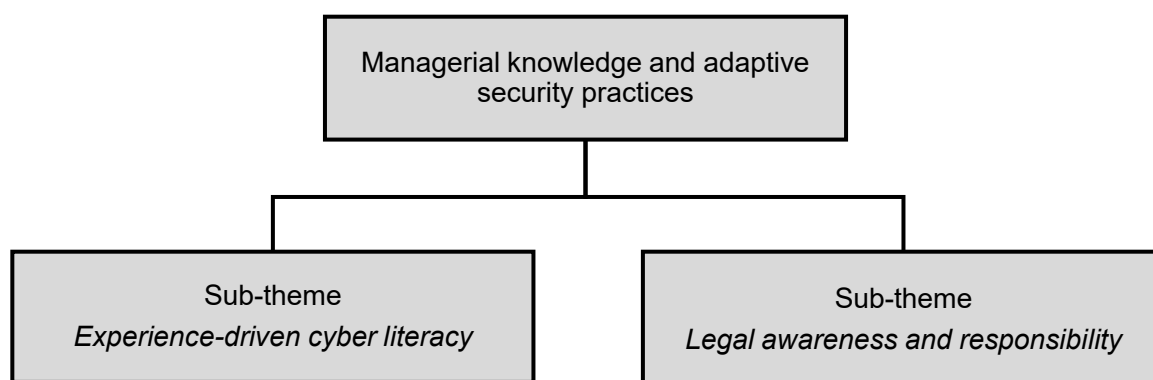


Figure 5. Themes that emerged from the research objective: Investigate the extent of comprehension and awareness of privacy/security principles

Sub-theme 3.1. Experience-driven cyber literacy

This theme suggests that SMEs accumulate their knowledge base through an iterative process of trial and error. This learning-by-doing approach generated a series of risk mitigation practices, including data backup, secure credential handling and selective platform use:

“I’ve built a routine for backups, secure passwords, encryptions, even if I never studied cybersecurity.” – Participant G

“Everything I know about cybersecurity, I learned by doing, not in a classroom.”
– Participant K

“Small lessons over time helped us develop practical routines like backups and stronger passwords.” – Participant A

These quotes highlight what might be regarded as *tacit digital competence*: the type of knowledge-in-action that is not formally accredited or externally mandated but that works well in routine business situations. Such bottom-up learning strategies suggest interventions in the future that utilise, rather than undermine, the experiential knowledge of SMEs.

Sub-theme 3.2. Legal awareness and responsibility

There is an evolution in the increasing legalisation of data protection through legal agreements and standardisation of protocols. The participants reported using non-disclosure agreements (NDAs), in-house privacy briefings and onboarding procedures to ensure security compliance among partners and customers:

“Before anyone touches our products, we go over privacy terms. NDAs are standard now.” – Participant D

“We started using NDAs and data clauses to stay ahead legally and ethically.”
- Participant J

Having something in writing reassures both our team and clients that we take data seriously.” - Participant L

This indicates a shift from responding to anticipating. Where leaders of SMEs are not merely technically adaptable but also institutionally accountable and establish trust. Such a shift demonstrates a broader understanding that data protection does not require sophisticated cybersecurity measures but rather extensive employee training and cooperation with external experts to ensure maximum protection (Siponen & Vance, 2018:92). In line with Sub-theme 3.1, which discusses cyber literacy gained

through practical experience, it appears that the majority of SMEs build their cybersecurity knowledge incrementally through experiential learning. By so doing, they accumulate what can be characterised as tacit digital knowledge. One example of top-down learning is that of Participant-G. They indicated embracing regular backups, robust passwords and encryption without the benefit of specialised cybersecurity training. Such practical knowledge is essential in CSA, where institutional support and training are officially absent and SMEs face resource deficiencies and limited availability of cybersecurity experts (Tikkinen-Piri *et al.*, 2018:279). However, SMEs demonstrate resilience through the application of basic security measures such as firewalls, anti-virus protection and using chosen platforms which provide risk minimisation within their resources (Nkomo & Mashiane, 2020:104).

Legal awareness and responsibility (sub-theme 3.2) are happening concurrently with learning by doing. SMEs have adopted standard operating procedures and legal contracts to formalise data protection. The quote from Participant D illustrates the shift from reactive to proactive cybersecurity strategies. These measures include the adoption of NDAs, internal privacy briefings and onboarding procedures. This institutionalisation fosters accountability and trust-building with clients and partners. Ultimately, this reinforces the ethical and reputational imperatives of privacy management. This is supported by Siponen and Vance (2018:92), who emphasise that embedding legal and procedural safeguards is essential for adequate data protection and organisational resilience.

However, financial constraints and doubt over technology suppliers continue to hinder the widespread adoption of sophisticated cybersecurity technology among SMEs (Puhakainen & Siponen, 2017:118). Still, the responsive behaviours observed where applied cyber literacy is merged with heightened legal awareness indicate that SMEs actively embrace viable and contextually relevant security measures. This dual strategy not only further improves day-to-day operational security but also sets the stage for further institutionalised policy-driven cybersecurity configurations.

The findings demonstrate a dynamic interaction of adaptive institutional practices and experiential learning in SMEs. Relying on their tacit knowledge and progressively formalising legal duty, SMEs in CSA are forging a resilient cybersecurity culture that involves technical, ethical and reputational considerations. Future initiatives may take

advantage of this strength. This provides SMEs with inexpensive solutions for training, hands-on experience and mitigating resource limitations and improving overall security.

3.3.4 Theme 4. Cultural and political contexts of trust

Compared to technical solutions, digital trust is firmly rooted in political and cultural meaning. Theme 4 illustrates how South African SMEs perceive cybersecurity as a means to enhance national sovereignty and foster communal solidarity. Depicted in Figure 3.4, this theme has two important sub-themes: the importance of having control over digital infrastructure and the role of *Ubuntu* as a normative guide for collective innovation.

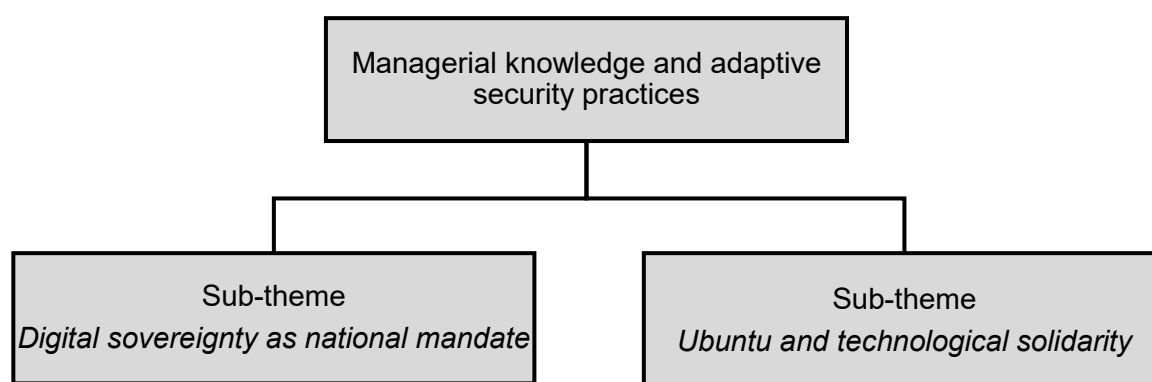


Figure 6. Themes that emerged from the research objective: Assess how cultural forces affect the way managers view and feel about privacy and security

Sub-theme 4.1: Digital sovereignty as a national mandate

The participants frequently expressed concern over foreign control of key digital infrastructure. They highlighted that this is not only a business concern but also a question of national autonomy:

“We’ve seen what happens when countries block each other. Imagine if we hosted everything locally, those shutdowns wouldn’t scare us.” – Participant I

“There’s a growing awareness that we need local control of digital infrastructure.” - Participant A

“I’d prefer South African hosting if it meant better privacy laws and autonomy.”

- Participant E

This response reveals a shift from individual risk assessment of SMEs to national risk consciousness. The participants perceived dependence on foreign digital platforms as a weakness that undermines resilience and confidence.

Sub-theme 4.2: Ubuntu and technological solidarity

Beyond geopolitical interests, the participants invoked the Ubuntu ethos to express their commitment towards building co-operative technological solutions. The emphasis was on self-determination, lateral cooperation and empowering people through digital technology:

“We developers have to unite, not wait for the government. We can do something better if we unite.” – Participant F

“There’s a spirit of collective effort in solving digital challenges together.” - Participant E

“We help each other when one of us learns something about online risks, we share it.” - Participant J

“Ubuntu also means we build each other’s resilience, especially in tech matters.” - Participant I

Ubuntu, in this instance, operates as a value that transcends culture. It is now a technology ethic that allows bottom-up innovation and open knowledge exchange. This collaborative approach presents a compelling counter-narrative to top-down digital governance models. This highlights the influence of communal solidarity on technology adoption and use. Based on the Unified Theory of Acceptance and Use of Technology (UTAUT2) (Venkatesh *et al.*, 2012:157), acceptance of technology is not only influenced by performance expectancy and effort expectancy but also social influence and facilitating conditions in the context of South African SMEs. Ubuntu is a powerful social force that encourages collaborative engagement with digital technologies. It fosters a shared sense of responsibility and peer-to-peer support in cybersecurity practices.

Sub-theme 4.1, Digital sovereignty as a national mandate, integrates performance expectancy and facilitates conditions in the UTAUT2 model. The participants' concerns about foreign control of cyber infrastructures reflect a desire for greater local control in ensuring reliability, resilience and trust. Perceived belief in the decrease of exposure to international political tensions when data is locally stored indicates the determinant of infrastructural and environmental factors over SMEs perceptions towards cybersecurity. This nationalistic construction lifts digital sovereignty from a technical choice to a strategic imperative that guides technology adoption and risk management decisions.

Sub-theme 4.2, Ubuntu and technological solidarity align with the social influence construct of UTAUT2. The reference to Ubuntu as a call for self-reliance and collaboration is symbolic of how collective innovation and knowledge sharing can be led by cultural standards and communal values. This social dynamic creates an enabling environment where SMEs feel empowered to co-develop solutions. It addresses the limitations imposed by external governance structures. It also reinforces the importance of developing conditions such as community networks and shared platforms. These platforms support the use of technology and promote security awareness. These sub-themes suggest that the trust in the digital platforms among South African SMEs is deeply rooted in political and cultural meanings. These significantly influence their technology acceptance behaviour. Interpreting these influences using the UTAUT2 framework provides a comprehensive understanding of how performance expectations, social and environmental conditions combine to influence the participation of SMEs in cybersecurity. This understanding suggests that effective cybersecurity responses in the CSA region are not simply intended to address technical competencies, but they also promote collective values and national aspirations to forge a strong digital future.

3.3.5 Theme 5: Sentiment and emotional orientation to risk

Theme 5 highlights the emotional and psychological aspects of cybersecurity engagement. The behaviours of managers of SMEs are not only influenced by knowledge or capacity but also by affective drivers such as fear and optimism. Figure 3.5 shows how this theme encompasses the emotional factors that influence digital decision-making, ranging from strategic caution to entrepreneurial resilience.

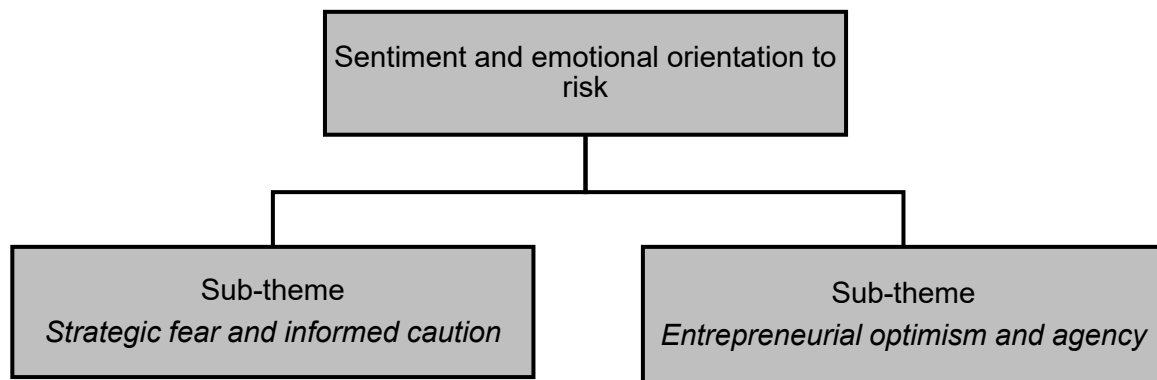


Figure 7. Themes that emerged from the research objective: review opinions and concerns about privacy/security

Sub-theme 5.1: Strategic fear and informed caution

The participants frequently mentioned fear as a motivator for vigilance. They also mentioned developing security protocols in response to previous threats:

“I don’t take anything for granted. One mistake online can cost everything.” – Participant A

“Fear is part of what drives our caution; we know how fast things can go wrong.”
- Participant K

“Just because nothing happened yet doesn’t mean we’re safe, we act as if we’re always being watched.” - Participant L

Such responses illustrate affective rationality, a form of reasoning that stems from emotional awareness of risk rather than from formal models or compliance standards. Far from being irrational, fear catalyses preventative action and defensive strategies.

Sub-theme 5.2: Entrepreneurial optimism and agency

The participants highlighted their ability to remain proactive and innovative despite structural constraints. They emphasised creating tailored solutions without external assistance or formal tools:

“We can’t wait for change. We create our systems, protect our data.” – Participant G

“We don’t just worry about threats; we see opportunities to improve how we do things.” - Participant B

“Even without big budgets, we innovate in small ways to stay safe and grow.” - Participant M

Such optimism is a manifestation of a robust entrepreneurial agency. This indicates that SMEs are not merely risk absorbers but digital problem solvers with adaptive potential. This agency can be understood through the lens of Ajzen's Theory of Planned Behaviour (TPB) (1991:180). According to this theory, intentions for behaviour are influenced by attitudes, subjective norms and perceived behavioural control. SMEs with positive orientations towards cybersecurity and strong perceptions of control over their cyberspace initiate active behaviours under conditions of external constraint. A belief in their ability to develop context-appropriate security solutions increases their perceived behavioural control, encourages innovation and protection behaviours.

Moreover, the Technology Acceptance Model (TAM) (1989:319) helps predict how such entrepreneurs learn and adapt to cybersecurity technologies based on perceived usefulness and ease of use. Entrepreneurial optimism in CSA is a cause for readiness to adopt digital technology when seen as valuable and viable, even with resource constraints. This internal motivation to use technology aligns with TAM's core hypothesis that favourable attitudes towards technology are a foundation for acceptance and sustained usage.

Conversely, strategic fear and rational caution as described in Sub-theme 5.1, are addressed in the Protection Motivation Theory (PMT) (1975:98). The theory emphasises the importance of perceived threat severity and susceptibility to threats. It also highlights self-efficacy and response efficacy as predictors of protective behaviour. According to Participant A, *“One mistake online can cost everything”* best sums up increased threat appraisal leading to increased vigilant security practices. Fear, in this case, is a rational stimulus that causes SMEs to employ defensive actions

that reduce perceived threats. Fear does not replace rational choice but supplements it by influencing cautious behaviour.

These theoretical perspectives emphasise the affective and cognitive forces underlying cybersecurity participation in SMEs. The struggle between fear-driven caution and optimism-driven initiative gives rise to a well-balanced set of behaviours through which SMEs ensure they are protected against risks while creating solutions simultaneously. An understanding of such affective drivers is crucial for developing interventions tailored to the lived experiences of SMEs. This will, as a consequence, activate their entrepreneurial potential while mitigating their vulnerabilities and anxieties.

3.3.6 Theme 6: Tactical innovation and future-ready solutions

The final theme reflects the forward-looking attitudes of SMEs. It captures their capacity to generate context-relevant digital solutions even under resource limitations. Figure 3.6 provides a strategic overview of how SME leaders envision future cybersecurity improvements, rooted in collaboration, simplification and community relevance.

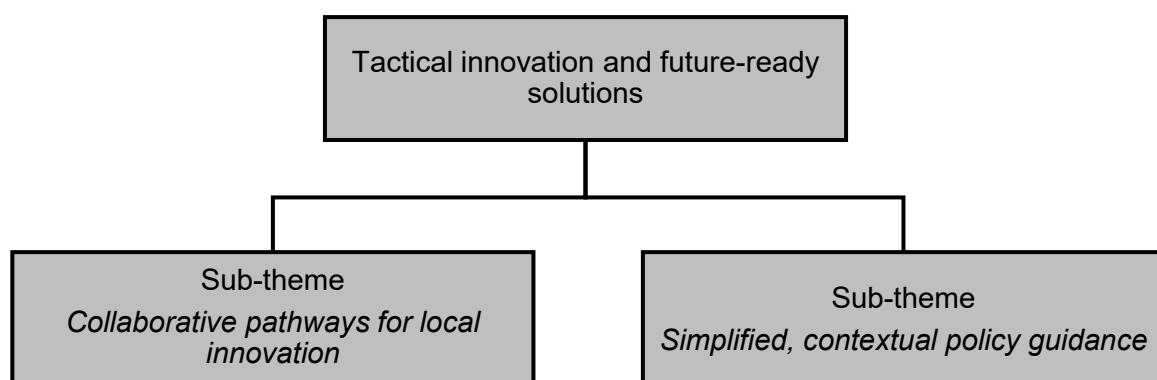


Figure 8. Themes that emerged from the research objective: Propose tactics to improve security/privacy protocols

Sub-theme 6.1: Collaborative pathways for local innovation

The participants identified several opportunities for home-grown solutions, including local hosting, developer forums and open-source collaborations. These initiatives were seen as vehicles for building digital sovereignty and self-reliance:

“Even without funding, we can start building. Between our networks, the knowledge is already here.” – Participant H

Forums where we can exchange ideas would help, mainly if they focus on real SME needs.” - Participant F

When developers and small businesses collaborate, we create more secure solutions.” – Participant I

This statement reflects a *grassroots innovation logic*, one that leverages community skills and social capital rather than external funding or government mandates.

Sub-theme 6.2: Simplified, contextual policy guidance

Despite the intense demands for innovation, participants were unhappy with the complex and incomprehensible regulatory policy guidelines. Participants concurred that they need usable, concise and graphical policy materials directed to the medium-sized enterprises context:

“We don’t need huge policies, just something short and practical, a guide made for us by us.” – Participant B

“We need policy guides that speak our language, not just legal jargon.” - Participant F

“If cybersecurity advice came in plain visuals or step-by-step formats, more people would follow it.” – Participant G

“Make the rules simple, clear, and local, then SMEs will adopt them.” - Participant H

This sub-theme shows the principle of usability over comprehensiveness. Practical cybersecurity guidance must be designed not just for accuracy, but also for accessibility and relevance. SMEs in the CSA region often face limited resources and lower levels of formal cybersecurity knowledge (Scholtz *et al.*, 2020:89). As a result, complex or technical policies can become barriers rather than enablers of good practice. This finding aligns with Siponen and Vance (2018:92), who emphasise that educating staff and providing clear, actionable protocols are essential components of

effective cybersecurity strategies. Simplified contextual policy guidance tailored to the unique needs of SMEs can empower them to implement protective measures with confidence and consistency.

Sub-theme 6.1 addresses the ways in which SMEs actively pursue local innovation collaborative paths. These include, for instance, developer forums, local data hosting and open-source projects. This logic of local innovation is one in a broader cultural and operating shift towards social capital and collective competency, mobilised to secure digital sovereignty and autonomy. Participant H's assumption that *"Even without funding, we can start building. Between our networks, the information is already here,"* illustrates the strength of peer learning and an informal mode of knowledge transfer. This collaborative approach aligns with the concept of ubuntu, previously discussed, where community innovation and horizontal cooperation are becoming increasingly normative drivers for the adoption of technology and problem-solving.

It also echoes the emphasis in the UTAUT2 (Venkatesh *et al.*, 2012:157) on social influence and facilitating conditions as key determinants of technology acceptance. Creating local networks and open-source projects enables SMEs to promote environments that counteract resource constraints. Furthermore, this creative thinking is supported by the need for simplified policy guidance (Sub-theme 6.2), which seeks effective instruments that take into account the real-world experiences of SMEs.

Even though they are necessary, advanced regulatory frameworks like POPIA can be intimidating if customised communication strategies are not used. Providing understandable and context-specific information can bridge the policy and implementation gap. It makes compliance less challenging and more manageable. These practices also encourage the development of a cybersecurity culture in which awareness and responsibility emerge naturally, rather than being imposed from the outside in South Africa. Together, these sub-themes capture a dual strategy for improving cybersecurity among SMEs in the CSA region. It is best for the catalysing of bottom-up, grassroots innovation to establish digital sovereignty and offer cost-free, user-centric policy guidance to facilitate effective governance. The discovery and advancement of these avenues can circumvent the structural and educational

challenges that currently prevent SMEs from engaging with cybersecurity. This eventually makes the digital economy more robust and sovereign.

3.4 Summary

The study reveals that perceptions and practices surrounding online privacy and security are shaped by a complex interplay of infrastructural dependencies, informal peer learning, cultural values and adaptive managerial behaviours. There is a lack of resources and institutional support among SMEs, making them rely on foreign cloud platforms. While these enhance business efficiency, they raise inherent concerns over data sovereignty and geopolitical risk. Peer networks substitute for a lack of formal cybersecurity education, resulting in innovation but sometimes technically limited risk-reducing responses. As these SMEs expand into digital commerce, they encounter new challenges regarding privacy concerns.

This extends beyond technical safeguards to encompass geopolitical anxieties and reputational risks, prompting a self-regulatory ethos focused on client trust and ethical stewardship. Managers in CSA have developed cyber literacy through experience, building routines such as data backups and secure credential management, while simultaneously formalising legal and procedural accountability through measures like NDAs and privacy briefings. Political and cultural influences, such as the desire for digital sovereignty and shared Ubuntu ethic also inform cybersecurity practices in CSA. This encapsulates both nationalist forms of infrastructure and shared, bottom-up innovation.

Other factors, such as fear, influence security behaviour, fuelling both entrepreneurial passion and strategic caution. Finally, the participants endorse locally relevant innovation strategies, such as developer forums and open-source communities. They also call for streamlined, context-relevant policy guidance that emphasises the need for practical and accessible resources rather than cumbersome regulatory regimes. These findings highlight the perceptions of managers in SMEs in addressing the multidimensional challenges of digital security within a resource-scarce and rapidly changing regional context.

CHAPTER 4: CONCLUSION AND RECOMMENDATIONS

4.1 Introduction

The objective of this chapter is to describe the key findings emanating from the qualitative research. The main aim of the study was to explore how SMEs in the CSA perceive and manage online privacy and security threats in the e-commerce context. This chapter describes the key findings of the study, offering pragmatic and policy-relevant recommendations and analysing the broader implications of the study. The chapter describes how the research objectives were achieved and provides the contributions of the study towards various scholarly and practical disciplines. The chapter describes the limitations associated with this study and offers suggestions for future studies. The study had the premise that cybersecurity and online privacy are not technically isolated issues, but rather multifaceted concepts with intersectionality in political, cultural, emotional and infrastructural constructs. Given that increasing numbers of South African businesses are adopting digital applications and platforms as part of their operational landscape, it is necessary to understand how they perceive and adapt to construct effective policy interventions and inclusive digital economies. Therefore, this chapter synthesises evidence into thematic conclusions to address the fundamental questions of how SMEs perceive and respond to cybersecurity challenges.

4.2 Summary of key findings

The research uncovered a complex and deeply contextualised understanding of cybersecurity among SMEs in CSA. One of the most compelling findings is that a confluence of infrastructural reliance, limited technical training, lived experiences and broader geopolitical sentiments shapes perceptions of digital risk. SMEs in urban centres such as Potchefstroom, Kimberley, Sasolburg and Kroonstad operate in semi-urban environments characterised by infrastructural imbalances and institutional cybersecurity deficiencies. In such conditions, entrepreneurs and managers rely primarily on their individual experience and informal networks to manage their businesses in the online environment.

The shared experience that was predominant is the dependency on international cloud providers such as Google Cloud, Amazon Web Services and Microsoft Azure. While

these services are developed to be efficient, scalable and integrable, they are hosted in a foreign jurisdiction that carries geopolitical risk. This can be felt as what might be called “*jurisdictional anxiety*.” This raises concerns regarding data held beyond South African jurisdiction, which is susceptible to data confidentiality breaches.

SMEs were lacking formal training in security protocols; therefore, they had to rely on peer-to-peer learning and experiential stories told by their peers. The participants recounted stories of data losses experienced by colleagues or competitors, which in turn motivated them to adopt more robust backup strategies or data minimisation techniques. This informal knowledge system can be considered adaptive and situated. However, it can also be superficial in terms of technical content. Nevertheless, it was much valued for being immediate, credible and proximal in cultural terms.

Another crucial finding pertains to how the participants interpret and deal with reputational risks. Cybersecurity was as much a matter of not losing client trust and safeguarding business reputation as it was about preventing technical breakdowns. Some participants had designed minimalist data collection strategies specifically to mitigate the reputational damage that could result from a breach. This self-regulatory impulse, not solely legislative compliance but rather moral compulsion, demonstrates how data privacy and protection have become intrinsic to the conduct of professionalism and reliability in SMEs in CSA.

Leadership knowledge was also characterised by trial-and-error learning. The participants reported having acquired their digital competencies not through formal instruction but through repetitive hands-on interaction with systems and applications. Nevertheless, these experiences translated into practical routines such as scheduled backups, careful password management, use of encryption tools and regular updates. At the same time, a new legal consciousness is seen through the use of NDAs, high-quality client onboarding processes and privacy briefings on the intranet. These sorts of institutional reforms are signs of a new cybersecurity culture, although these reforms do not enjoy systemic support.

Political and cultural frames were key in describing how SMEs feel and push back against risk. Digital sovereignty was highlighted with participants demanding that South Africa specify its digital infrastructure. This was not mere nationalism, but the belief in the capacity of the local and the need to shift from reliance on foreign digital

platforms. Besides that, Ubuntu philosophy played a crucial role, more as a principle of working rather than as a moral call to action, for community innovation, cross-pollination and sharing of infrastructure. The participants highlighted cooperative development models, i.e., open-source initiatives and local developer communities to produce inclusive cyber-defence approaches.

4.3 Conclusion

The study concludes that SMEs in the CSA approach cybersecurity through an intricate matrix of practical experience, cultural resonance, political consciousness and emotional intelligence. While constrained by infrastructural limitations and the absence of formal cybersecurity education, these businesses demonstrate remarkable resilience, adaptability and innovation in their approach to interpreting and responding to online risks. Far from passive recipients of the digital context, SMEs in CSA are active agents of their technology, constructing their knowledge systems, developing normative guidelines and advocating localised responses. The study underlines the importance of recognising cybersecurity as not only a technical discipline, but as a human, cultural and political practice. Cybersecurity engagement is often embedded in ethical commitments to clients, communal solidarity and national development narratives. Business owners and managers mobilise personal networks, emotional experiences and grassroots strategies to construct a protective digital environment that reflects both their constraints and their aspirations.

4.4 Recommendations

The findings reveal where interventions should occur and can be applied to enhance the cybersecurity position of SMEs in the CSA region. Any interventions should be based on the socio-economic, infrastructural and cultural needs of the subject companies. The recommendations expounded herein are not prescriptions or universally applicable principles. Still, they are adapted to the day-to-day reality, limitations and aspirations of SMEs as expressed by their managers and owners.

4.4.1 Contextual, visual policy tool development

The ventilated frustration by the participants regarding the technicality and complexity of modern-day cybersecurity regulations highlights a need for simplified and context-

specific direction. SMEs require better than theoretical legislation; they require interpretive tools that demystify national or global cybersecurity guidelines into applicable, comprehensible and locally relevant guidelines. Therefore, regulatory bodies and industry sectors need to join forces with practitioners to collaborate in creating visually centred cybersecurity toolkits that comprise infographics, checklists, flowcharts and brief explanatory videos articulating key principles and practices in easy language.

These resources should be provided not only by official online portals, but also by sector associations, local development forums and chambers of commerce that SMEs already trust. These policy tools must be piloted and designed with the participation of end-users in order to ensure that they are consistent with the operating logic and cognitive frame of the target group. This participatory approach will foster greater ownership, enhance uptake and establish trust in the regulatory framework.

4.4.2 Local hosting and infrastructure development

Given the widespread concern over foreign data dependency, national and provincial governments must prioritise the promotion of locally hosted digital infrastructure. This includes incentivising the development of secure data centres in South Africa and encouraging public procurement policies that favour local cloud providers. Government-sponsored infrastructure investment, possibly through public-private partnerships can provide steady alternatives to foreign platforms while maintaining data in South African jurisdiction. This will then address the '*jurisdictional concern*' that most SMEs have.

Moreover, municipalities can grant tax exemptions or subsidised digital services to SMEs when they transition to locally hosted platforms, not merely as a question of principle but also an economically viable choice. Universities and technical colleges could be enlisted as implementation partners, helping to build and manage small-scale data ecosystems in semi-urban centres such as Potchefstroom and Kimberley.

4.4.3 Strengthening peer-led cybersecurity training

Many SME managers acquired their knowledge through peer networks and practical experimentation. Formal training programmes should build on this existing grassroots ecosystem rather than replace it. Industry associations, regional development

agencies and universities ought to promote the formation of peer-led cybersecurity learning groups, where managers can share experiences, explore case studies and co-design best practices for their specific sectors.

Rather than lecture-based content transmission, these groups need to prioritise dialogic learning, simulations and scenario-based practice reflecting everyday business tasks, such as client onboarding or the use of cloud-based accounting platforms. Where possible, these sessions need to be conducted by practitioners who are the members of the community. This will enhance relatability and trust. Financial support needs to be provided to ensure that participation does not impose operational downtime.

4.4.4 Including cybersecurity in business support curricula

Existing business support services need to include cybersecurity modules in their standard training programmes. The modules should not only introduce primary technical concepts such as encryption and multi-factor authentication, but also cover the ethical, legal and reputational dimensions of data stewardship. For example, sessions might examine the role of privacy in sustaining customer trust or how NDAs and onboarding protocols can mitigate contractual risk.

Cybersecurity should be taught not as a discrete technical discipline, but as an essential component of sound enterprise management and a key to achieving competitive advantage. Linkages should be established between cybersecurity and financial planning (e.g., cost of breach scenarios), branding (e.g., reputational resilience) and operations (e.g., system downtime and recovery planning). This will therefore position cybersecurity as an integrated business function.

4.4.5 Building innovation ecosystems through local developer forums

The participants' call for collective innovation rooted in the spirit of Ubuntu presents a unique opportunity to cultivate localised cybersecurity solutions. Municipalities, business chambers and tech hubs should co-host developer forums and open-source collaboration platforms where small development teams, security experts and business owners can co-create tailored digital tools. These might include sector-specific risk assessment templates, client-facing privacy banners or intrusion detection scripts adapted for local conditions.

Such forums would also serve as trust-building spaces in which SMEs from different industries can share their needs and co-learn. This will therefore reduce duplication and enhance cost efficiency. For example, a developer who creates a secure inventory system for a local retailer might find their solution easily adaptable to the logistics or agri-processing sector. This spirit of trans-sectoral collaboration represents a distinct South African response to the global cybersecurity challenge.

4.4.6 Promoting cybersecurity through public awareness campaigns

Beyond enterprise-level intervention, a broader public discourse on cybersecurity is required, one that normalises discussion of data protection, raises public expectations of business accountability and strengthens societal trust. National and provincial governments, in partnership with civil society, should develop awareness campaigns that spotlight everyday cybersecurity issues using culturally resonant language and storytelling formats.

4.5 Achievement of study objectives

This study successfully achieved its objectives. It examined the factors influencing SMEs' perceptions of online security and privacy. It also explored their perceptions regarding e-commerce security, client trust and ethical data practices. The secondary objectives were equally satisfied. The study provided an analysis of SMEs' perceptions across diverse urban and semi-urban towns in CSA, explored managerial knowledge acquisition in cybersecurity contexts and unpacked the cultural and political factors, including ubuntu and digital sovereignty that influence risk perceptions. Moreover, it presented a grounded account of the landscape of cybersecurity engagement and concluded with practical, tailored recommendations for policy and enterprise action. Table 4.1 provides a summary of how each research objective was achieved.

Table 4.1. Achievement of study objectives

Objective	How the Objective was achieved in the study
Examine the factors that influence business perceptions • Elements that affect how businesses in CSA perceive online privacy and security risks	The study found that perceptions were influenced primarily by infrastructural reliance (especially on global cloud platforms), peer experiences and informal learning.
Evaluate perceptions of privacy and security risks • How managers in SMEs view online shopping privacy/security	SMEs were concerned about jurisdictional risks (e.g., foreign surveillance) and managing client trust. Strategies such as data minimisation were adopted to mitigate risks.
Assess business perceptions • Perspectives of businesses in CSA on e-commerce security/privacy • Focus on SMEs in specific urban/semi-urban areas	SMEs across CSA locations (e.g., Bloemfontein, Sasolburg, etc.) reflected diverse, but consistent awareness of online privacy and security, influenced by locality, infrastructure and access to knowledge.
Understand managerial knowledge • Awareness of privacy/security principles • Concerns and perspectives	SMEs demonstrated cyber literacy gained through practical experience, complemented by emerging legal accountability measures (e.g., NDAs, internal policies).
Cultural impact analysis	Cultural concepts like <i>Ubuntu</i> and nationalistic concerns about <i>digital sovereignty</i> were significant influences on how SMEs approached cybersecurity.

• Effect of cultural forces and political environment on perceptions	
Sentiment reviews • Opinions/concerns of business executives • Factors affecting understanding and behaviours	Emotional factors such as <i>fear</i> , <i>caution</i> and <i>entrepreneurial optimism</i> shaped security behaviours. These sentiments drove both protective routines and innovation.
Practical recommendations • Propose tactics to improve protocols based on research findings	The participants suggested local innovation (developer forums, local hosting) and called for <i>simple</i> , <i>practical</i> and <i>contextual</i> cybersecurity policy guidance.

Boqo, X. (2025). Researcher's own compilation from synthesis of research findings.

4.6 Contribution of the Study

The following sections describe the contributions made by this study.

4.6.1 Contribution to Policymakers

The study provides robust empirical support to inform the formulation of public policy in digital governance. The study demonstrates that cybersecurity policy must go beyond compliance measures to include accessibility, cultural sensitisation and context sensitivity. Policymakers are encouraged to design modular policy instruments that can be deployed in various regions with varying infrastructure capacities. The evidence also highlights the importance of investment in local hosting and cybersecurity innovation spaces in the development of national digital resilience and sovereignty.

4.6.2 Contribution to small and medium-sized enterprises

For SMEs, the study provides a helpful comparative and reflective understanding of how peer businesses function in the cybersecurity context. It legitimises bottom-up knowledge systems and provides an analytical framework through which managers can compare their processes. It also provides solutions and conceptual tools to enable better self-regulation, institutional accountability and protection of organisational reputation. The study findings enable SMEs to perceive cybersecurity as an opportunity rather than a cost, to exercise ethical leadership and competitive distinction.

4.6.3 Contribution to literature

This study adds information that is different to the academic literature on cybersecurity, especially when it comes to how SMEs in the global South deal with cybersecurity. Rather than centring on frameworks built in Silicon Valley boardrooms or corporate IT departments in the global North, this research focuses on the lived experiences of SMEs in CSA, navigating real-world digital risks with resourcefulness and grounded resilience.

For a long time, much of the cybersecurity literature has focused on technical solutions designed for large organisations with access to expertise, infrastructure and policy support (Bada *et al.*, 2019; Von Solms & Van Niekerk, 2013). This study deliberately breaks away from that narrative. It shows that online security in semi-rural South Africa is not certificates and firewalls. Instead, it is trust, community, trial and error and

improvisation. The findings are consistent with Aurigemma and Mattson (2019), who also acknowledge informal, social knowledge as having a critical role in shaping cybersecurity practice among SMEs.

This research also provides room for more emotionally and culturally sensitive technology adoption models. Conventional models like TAM (Davis, 1989) and UTAUT2 (Venkatesh *et al.*, 2012) have conventionally guided discussions of why particular technologies have been adopted. However, this study shows that cybersecurity choices are not simply an issue of usability or usefulness but are also an outcome of more basic issues of data sovereignty, human agency and local values like Ubuntu. It is a challenge to recreate these models through a more rooted Southern lens, consistent with the research by Ali and Osmanaj (2020), who were the first to adapt these theories to regulatory and cultural intricacy.

Another significant contribution is how this research teases out the unrevealed ethics of data protection that businesses observe not out of law, but out of relation. Similar to Jones (2022:218), it shows that for many SMEs, protecting customer information is not just a best practice. It is about reputation, trust and doing right by the people served by businesses. What this study contributes is a higher resolution of that ethical urge: the self-control of collecting only what is necessary, creating NDAs and training employees on privacy procedures even when no one is watching.

It also applies theories like Protection Motivation Theory (Rogers, 1975) and the Theory of Planned Behaviour (Ajzen, 1991), in showing that fear, when constructive and informed, can mobilise businesses into action. The participants were not paralysed by fear, but were mobilised to take control. In addition, their fear and hope generated creative, locally designed solutions. The combination of hope and fear provides a more emotionally engaged means of considering security behaviour, building on Bada *et al.*'s (2019) awareness campaign and individual agency research.

Finally, whereas national cybersecurity strategies often focus on centralised infrastructure or top-down regulation (Von Solms & Van Niekerk, 2013), this study argues for a more grassroots approach. It demonstrates how communities of practice, developer groups, peer learning networks and even WhatsApp chat groups can be just as effective in constructing resilience. It proposes specific alternatives: distilled policy guides, visual

toolkits and digital partnerships founded on Ubuntu. This vision not only fills a gap in the literature but also reshapes the way to envision successful, inclusive cybersecurity throughout the continent.

4.7 Limitations of the study

Although the study presents an empirically rich and illustrative picture of cybersecurity in SMEs in CSA, it has some limitations. The geographical focus was confined to urban and semi-urban towns in a specific region that comprised Bloemfontein, Potchefstroom, Sasolburg and Kimberley, among others. Thus, the findings may not necessarily apply to the exact conditions of enterprises in more rural or very high-density urban areas, such as Johannesburg or Cape Town, where access to digital networks and institutional capital might be substantially different.

Secondly, the study relied on qualitative information gathered through semi-structured interviews. While this was possible in an effort to offer depth and background, it also imposes restrictions on generalisability. The individual views of a relatively small sample, yet varied by industry and knowledge level, may not accurately reflect general trends in SMEs throughout South Africa. Follow-up studies can complete these findings with quantitative measurement, e.g., questionnaires or risk assessment to validate emergent themes at an aggregate level.

The investigation did not encompass observational data and longitudinal analyses of behaviour change over time. These findings provide only a snapshot of perceptions at a particular moment.

Lastly, the research design did not incorporate client perspectives. Since trust and privacy of client information turned out to be central themes, the incorporation of the voices of consumers dealing such businesses would have been insightful in this regard on how privacy is being negotiated at both ends of the digital value chain.

4.8 Suggestions for future studies

There are several interesting avenues for further research based on the framework established by this study. Comparative studies across industries and provinces to explore how variations in the regulatory, sociocultural and infrastructure contexts affect

cybersecurity practices. Future studies could reveal differences at the national level and help shape more regionally focused digital policies.

Longitudinal studies can also explore how managerial attitudes and organisational practices evolve over time. They can also explore how regulatory frameworks such as the POPIA are implemented or how consumer attitudes change. Tracking change in real time could have more actionable implications for practitioners and policymakers.

In addition, there is potential to explore client-side experiences; namely, how trust is established and maintained in online transactions with SMEs. The consumer's perspective of data protection may be utilised to inform us about more balanced, co-produced models of cybersecurity that considers both sides of the transaction.

Finally, it would be informative to examine the gendered politics of cybersecurity leadership and participation in SMEs regarding the use of personal networks.

REFERENCE LIST

- Abawajy, J. 2014. Determining malicious activities in network traffic using lightweight security framework. *Security and Communication Networks*, 7(1):115-129.
- Ajzen, I. 1991. The theory of planned behaviour. *Organizational Behaviour and Human Decision Processes*, 50(2):179-211.
- Ali, O. & Osmanaj, V., 2020. The role of government regulations in the adoption of cloud computing: An empirical study of the impact of GDPR on cloud adoption in the UK. *Government Information Quarterly*, 37(3), p.101486.
- Aloul, F.A. 2019. The need for effective information security awareness. *Journal of Advances in Information Technology*, 10(1):45-53.
- Arora, S., Kar, A. & Dwivedi, Y.K. 2021. Understanding consumer adoption of mobile payment in India: Extending the meta-UTAUT model with personal innovativeness, anxiety, trust, and grievance redressal. *International Journal of Information Management*, 56:102-123.
- ATLAS.ti Scientific Software Development GmbH. 2023. ATLAS.ti for Windows, Version 24. Berlin, Germany: ATLAS.ti GmbH.
- ATLAS.ti. (n.d.). Qualitative data analysis with powerful software tools. Available at: <https://atlasti.com/guides/qualitative-research-guide-part-2/qualitative-data-analysis-software>. Date of access: 23 January 2024.
- Aurigemma, S. & Mattson, T. 2019. Do It OR ELSE! Exploring the effect of coercion on organizational users' compliance with information security policies. *European Journal of Information Systems*, 28(4), pp.395–412.
- Aurigemma, S. & Mattson, T. 2019. Exploring the antecedents of employees' information security policy compliance decisions: Validating the information security awareness construct. *Decision Sciences*, 50(2):379-426.
- Babbie, E. 2020. The practice of social research. 15th ed. Boston: Cengage Learning.

Bada, M., Sasse, A. & Nurse, J.R.C., 2019. *Cyber Security Awareness Campaigns: Why do they fail to change behaviour?* arXiv preprint arXiv:1901.02672.

Bansal, G., Zahedi, F.M. & Gefen, D. 2016. The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. *Decision Support Systems*, 49(1): 980-991.

Barney, J. 1991. Firm resources and sustained competitive advantage. *Journal of Management*, 17(1): 99-120.

Berger, R. 2015. Now I see it, now I don't: Researcher's position and reflexivity in qualitative research. *Qualitative Research*, 15(2): 219-234.

Black, R. 2018. *Subtle influences: How online environments shape decisions*. New York: Digital Press.

Boss, S.R., Galletta, D.F., Lowry, P.B., Moody, G.D. & Polak, P. 2020. What do users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly*, 43(1): 289-312.

Botha, E. & Van Zyl, G. 2017. Investigating Online Security and Privacy in South Africa: A conceptual overview. *South African Journal of Information Management*, 19(1): 78 – 89. Available at: <https://sajim.co.za/index.php/sajim/issue/view/56> Date of access: 26 Nov. 2023.

Boqo, X. 2025. Field interview data on factors influencing business perceptions of online privacy and security risks in Central South Africa. Unpublished raw data. North-West University Business School, Potchefstroom.

Boqo, X. 2025. Synthesis of findings from field data on factors influencing business perceptions of online privacy and security risks in Central South Africa. Unpublished mini-dissertation data. North-West University Business School, Potchefstroom.

Boqo, X. 2025. Thematic analysis of interview data on factors influencing business perceptions of online privacy and security risks in Central South Africa. Unpublished raw data. North-West University Business School, Potchefstroom.

Braun, V. & Clarke, V. 2006. Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2): 77-101. Available at: https://www.researchgate.net/publication/235356393_Using_thematic_analysis_in_psychology. Date of access: 22 September 2023.

British Psychological Society. 2018. Code of Ethics and Conduct. Available at: <https://www.bps.org.uk/guideline/code-ethics-and-conduct>. Date of access: 03 October 2023.

Brown, A. & Johnson, L. 2018. Online Retail in South Africa: An Overview. *Journal of South African Commerce*, 12(3): 45–60. Date of access: 22 September 2023.

Brown, J. & Anderson, L. 2021. *Methodologies in Modern Research*. Portico Publishing.

Brown, S. 2023. Privacy paradox: Data Collection and User Concerns in the Digital Age. *International Journal of Cybersecurity*, 29(1): 56-80.

Brown, T. 2020. The role of platform managers in data privacy and security: An exploratory study. *Journal of Business and Information Systems*, 13(1): 25-34.

Bryman, A. 2016. *Social Research Methods*. Oxford: Oxford University Press.

Bryman, A., Bell, E., Dos Santos, A., Du Toit, J., Hirschsohn, A., Masenge, A. & Wagner, C. 2014. *Research Methodology: Management and Business Contexts*. Oxford: Oxford University Press.

Bulgurcu, B., Cavusoglu, H. & Benbasat, I. 2010. Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, 34(3): 523-548.

Chaffey, D. & Ellis-Chadwick, F. 2019. *Digital Marketing*. London: Pearson.

Chen, C. 2019. SME adoption of internet security practices. *Journal of Cyber Security Technology*, 3(2):64-78.

Chen, S., Wang, Z. & Li, N. 2019a. Cybersecurity Incidents and Customer Trust: A Longitudinal Study. *Journal of Information Security*, 25(3): 45-60.

Chen, Y., Zhang, X., & Xu, Y. 2019b. Privacy concerns, perceived assurance, and online purchase intention: The moderating effect of risk awareness. *Journal of Retailing and Consumer Services*, 49: 72 – 81.

Clarke, R. 2010. *Encyclopaedia of E-Commerce Development, Implementation and Management*. Hershey, PA: IGI Global.

Creswell, J.W. & Creswell, J.D. 2018. *Research Design: Qualitative, Quantitative, and Mixed Methods Approach*. Thousand Oaks, CA: Sage Publications.

Creswell, J.W. 2013. *Research Design: Qualitative, Quantitative and Mixed Methods Approach*. Thousand Oaks, CA: Sage Publications.

Creswell, J.W. & Creswell, J.D. 2018. Research design: qualitative, quantitative, and mixed methods approaches. 5th ed. Thousand Oaks, CA: SAGE Publications.

Crouch, M. & McKenzie, H. 2006. The logic of small samples in qualitative research based on interviews. *Social Science Information*, 45(4): 483 – 499. Available at: <https://journals.sagepub.com/doi/abs/10.1177/0539018406069584>. Date of access: 10 October 2023.

Davies, M. 2021. *Communication and Digital Trust*. Cape Town: Digital Trust Publications.

Davis, F.D. 1989. Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 13(3): 319-340. Available at: <https://www.jstor.org/stable/249008>. Date of access: 13 November 2023.

Davis, M. & Thompson, S. 2017. Digital Privacy and Security: Contemporary Analysis. *Journal of Cybersecurity*, 8(2): 120-135.

Department of Justice and Constitutional Development. 2013. *Protection of Personal Information Act, No. 4 of 2013*. Government Gazette, 37067(798): 1-103.

DiCicco-Bloom, B. & Crabtree, B.F. 2006. The qualitative research interview. *Medical Education*, 40(4): 314-321. Available at:

<https://asmepublications.onlinelibrary.wiley.com/doi/pdf/10.1111/j.1365-2929.2006.02418.x>. Date of access: 15 October 2023.

Dissmann, J. 2004. E-Commerce in Africa: Challenges and Opportunities. *International Journal of Electronic Commerce*, 8(1): 73-89.

Dlamini, M.T., Eloff, J.H.P. & Eloff, M.M. 2019. Information security: Compliance to the protection of personal information act. *Information Systems Frontiers*, 21(1): 139-146.

Dlamini, Z. 2016. *Consumer trust in e-Commerce: A South African perspective*. Pretoria: University of Pretoria Press.

FinMark Trust. 2020. *FinScope MSME Survey South Africa 2020*.

Flick, U. 2018. *An Introduction to Qualitative Research*. 6th ed. London: Sage.

Free State Provincial Government. 2021. Economic Overview of the Free State. Retrieved from <https://www.freestate.gov.za/economy> Date of access: 19 June 2024.

Free State Tourism. 2019. Discover Parys. Retrieved from <https://www.freestatetourism.org/parys> Date of access: 19 June 2024.

Furnell, S. & Karweni, T. 2007. Security implications of electronic commerce: A survey of consumers and businesses. *Computers & Security*, 26(4): 289 – 304. Available at: <https://www.emerald.com/insight/content/doi/10.1108/10662249910297778/full/html> Date of access: 10 November 2023.

Gauteng Provincial Government. 2017. Industrial development in Vanderbijlpark. Retrieved from <https://www.gauteng.gov.za/industries> Date of access: 19 June 2024.

Gefen, D., Karahanna, E. & Straub, D.W. 2018. Trust and TAM in online shopping: An integrated model. *MIS Quarterly*, 42(2): 407-430.

Gordon, L.A., Loeb, M.P. & Zhou, L. 2018. The impact of information security breaches: Has there been a downward shift in costs? *Journal of Computer Security*, 26(3): 55-85.

Government of South Africa. (n.d.). About Bloemfontein. Retrieved July 1, 2024, from <https://www.gov.za/about-sa/provinces/free-state> Date of access: 19 June 2024.

Guest, G., Bunce, A. & Johnson, L. 2006. How Many Interviews Are Enough? An experiment with data saturation and variation. *Field Methods*, 18(1): 59–82.

Gupta, B. & Arora, R. 2019a. Privacy policy perceptions and concerns: A study of online users. *International Journal of Information Management*, 44: 65–75.

Gupta, N. & Arora, R. 2019b. Online privacy concerns: A broad overview. *Journal of Global Information Management*, 27(1): 117–139.

Hartman, D. 2015. Digital loyalty: Beyond transactions. *E-Commerce Reviews*, 6(1): 12 – 23. Available at: <https://fastercapital.com/content/Customer-loyalty-vision--Loyalty-Beyond-Transactions--Nurturing-Customer-Relationships.html> Date of access: 22 September 2023.

Hashemi-Pour, C. & Lutkevich, B 2023. e-commerce. CIO. Available at: <https://www.techtarget.com/searchcio/definition/e-commerce>. Date of access: 16 May 2024.

Hiranandani, V. 2011. Privacy and security in the digital age: Contemporary challenges and future directions. *The International Journal of Human Rights*, 7(15): 1091 – 1106. Available at: <https://www.tandfonline.com/doi/full/10.1080/13642987.2010.493360> Date of access: 26 Nov. 2023.

Hoft, J. (2021). Anonymity and confidentiality. *The Encyclopedia of Research Methods in Criminology and Criminal Justice*, 1, 223-227.

<https://www.niehs.nih.gov/research/resources/bioethics/whatis/index.cfm>

Saunders, M., Lewis, P. & Thornhill, A. 2019. Research methods for business students. 8th ed. Harlow: Pearson Education.

Ilyoo, B.H. & Hoon, S.C. 2013. The mediating role of consumer trust in an online merchant in predicting purchase intention, *International Journal of Information Management*, Elsevier, 33(6): 927 – 939. Available at:

<https://ideas.repec.org/a/eee/ininma/v33y2013i6p927-939.html> Date of access: 22 September 2023.

Johnson, L. 2010. *Understanding Literature Reviews: A Guide for the Modern Researcher*. London: Academic Press.

Johnson, L. 2020. *Trust and Online Retail in South Africa*. Johannesburg: SA E-Commerce Review.

Johnson, M. & Henderson, S. 2021. Trust in the age of data breaches: A managerial perspective. *Journal of Business Ethics*, 159(2): 543 – 558. Available at: https://www.researchgate.net/publication/357413774_Do_You_Still_Trust_The_Role_of_Age_Gender_and_Privacy_Concern_on_Trust_after_Insider_Data_Breaches Date of access: 22 Sep. 2023.

Johnson, R.B., & Christensen, L. 2008. *Educational Research: Quantitative, Qualitative, and Mixed Approaches*. Los Angeles: Sage.

Johnston, A.C., Warkentin, M. & Siponen, M. 2021. An enhanced fear appeal rhetorical framework: Leveraging threats to the human asset through sanctioning rhetoric. *MIS Quarterly*, 45(1):215-239.

Jones, A. & Smith, B. 2012. Theoretical underpinnings of online privacy perceptions. *Journal of Internet Behaviour*, 5(2): 45 – 62.

Jones, B. (2022). Is POPIA bad business for South Africa? Comparing the GDPR to POPIA and analyzing POPIA's impact on businesses in South Africa. *Penn State Journal of Law & International Affairs*, 10(1), 218.

Jones, K., Dasgupta, S. & Choo, K.K.R. 2019. A multivocal literature review of cybersecurity economics. *Information and Computer Security*, 27(2):105-121.

Kareem, T. & Johnson, L. 2021. Cybersecurity challenges for SMEs in Sub-Saharan Africa. *Cybersecurity Review*, 8(1):112-130.

Khumalo, B. 2018. *Measuring online behaviour: Tools and methodologies in South Africa*. Durban: UKZN University Press.

Khuzwayo, H. 2019. *Exploring digital landscapes: SMEs in the age of cybersecurity*. Durban: KZN Publishers.

Khuzwayo, W., Petersen, M. & Mthembu, L. 2018. *Digital Trust and SMEs in South Africa*. Durban: KZN Publishers: 22.

Kim, H. & Park, J. 2017. Building Trust in Online Platforms: The role of customer Interactions and Reviews. *Journal of Online Business*, 20(2): 78 – 95.

Kim, J. & Park, H. 2017. Effects of consumer privacy concerns on e-commerce: A meta-analysis. *International Journal of Information Management*, 37(1): 1 – 14. Available at: https://www.researchgate.net/publication/257252699_The_effect_of_online_privacy_policy_on_consumer_privacy_concern_and_trust Date of access: 10 Nov. 2023.

Kritzing, E. & Smith, M. 2021. POPIA compliance and its impact on e-Commerce platforms. *South African Journal of Information Management*, 23(1): a1521. Available at: <https://popia.co.za/> Date of access: 26 Nov. 2023.

Kritzing, E. & Von Solms, R. 2003. Information security management: A new paradigm. In Proceedings of the IFIP TC11 18th World Computer Congress, 301 –312. Available at: <http://www.sis.pitt.edu/jjoshi/courses/is2621/SecManParadigm2.pdf> Date of access: 2 Nov. 2023.

Kritzing, W.T. & Smith, E.E. 2021a. The Impact of POPIA on Electronic Commerce in Central South Africa. *South African Journal of Information Management*, 23(4): 1 – 15.

Kritzing, W.T. & Smith, E.E. 2021b. The Impact of Privacy Factors on Customer Trust in Online Platforms. *South African Journal of Business Management*, 45(2): 112.

Kritzing, W.T. & Smith, E.E. 2021c. Cybersecurity awareness and implementation in South African companies. *Computers & Security*, (98):101 – 973.

Lee, J. & Hong, S. 2022. Factors influencing information security behaviour in organisations: A South Korean perspective. *Journal of Cybersecurity*, 5(2):145-161.

Li, H., Sarathy, R. & Xu, H. 2018. The role of affect and cognition on online consumers' decision to disclose personal information to unfamiliar online vendors. *Decision Support Systems*, 51(3):134-145.

Liu, C., & Babar, M. A. (2024). Corporate cybersecurity risk and data breaches: A systematic review of empirical research. *Australian Journal of Management*, 03128962241293658.

Louw, J. 2020. Privacy in the digital age: Challenges and opportunities for South African businesses. *Journal of Information Privacy*, 7(1):64-79.

Maduku, D.K. 2021. Data privacy concerns in South Africa: Examining consumer understanding of the POPIA. *Journal of Consumer Marketing*, 38(2): 229-240.

Maree, K. 2019. Exploring the influence of cultural factors on cybersecurity practices in African businesses. *African Journal of Information Systems*, 11(4): 55-67.

Mathews, K. & Farnden, J. 2021. Cybersecurity in African small and medium enterprises: Challenges and responses. *African Journal of Business and Economic Research*, 16(1): 175-189.

Minister Lindiwe Zulu on achievements of Department of Small Business Development | Department of Small Business Development. 2017. Available at: <http://www.dsbd.gov.za/media-release/minister-lindiwe-zulu-achievements-department-small-business-development> Date of access: 2 May. 2024.

Miranda, J., Cortez, M. & Cortez, J. 2019. Digital transformation in medium enterprises: A case study of South African businesses. *Journal of Business Strategy*, 40(2): 50-55.

Mkhize, R. 2022. E-Commerce trends in Central South Africa. *South African Business Journal*, 45(2): 56 – 70.

Mokoena, L. 2019. Digital adoption among SMEs in central South Africa. *Bloemfontein Studies in Business*, 13(1): 10 – 29.

Mokoena, L. 2020. *Constructivist methodologies in the digital age*. Pretoria: Gauteng Academic Press.

Mokoena, T. & Botha, Z. 2020. *The Digital Landscape of medium-sized businesses in South Africa*: 28. Bloemfontein: Free State Publications.

Moriña, A. (2021). When people matter: The ethics of qualitative research in the health and social sciences. *Health & social care in the community*, 29(5), 1559-1565.

Mou, J., Shin, D.H. & Cohen, J.F. 2017. Trust and risk in consumer acceptance of e-services. *Electron Commer Res*, 17: 255 – 288. Available at: <https://doi.org/10.1007/s10660-015-9205-4> Date of access: 16 May. 2024.

Mugwagwa, A., Bhero, E. and Chibaya, C., 2024. Cybersecurity strategy: future proof cybersecurity for small to medium enterprises in South Africa. *International Journal of Research in Business and Social Science*, 13(4), pp.1524.

Ndlovu, M. 2018. *The Digital Consumer: Privacy perceptions and practices*. Bloemfontein: Free State Press.

NIST (National Institute of Standards and Technology). 2018. *Cybersecurity Framework: Improving Critical Infrastructure Cybersecurity*. [online] Available at: <https://www.nist.gov/cyberframework>. Date of access: 10 Oct. 2023.

Nkomo, C. & Mashiane, J. 2020. Information security management in South African SMEs: The challenges and solutions. *South African Journal of Business Management*, 51(1):99-107.

Nkosi, M. 2022. POPIA compliance among South African small and medium enterprises. *Journal of African Business*, 23(2):130-145.

North West Provincial Government. 2019. *Agricultural Activities in Lichtenburg*. Retrieved from <https://www.northwest.gov.za/agriculture>. Date of access: 19 June 2024.

North West University. 2020. Potchefstroom Campus Overview. Retrieved from <https://www.nwu.ac.za/potchefstroom>. Date of access: 19 June 2024.

Northern Cape Tourism Authority. 2020. Kimberley: The Diamond City. Retrieved from <https://www.northerncapetourism.co.za/kimberley>. Date of access: 19 June 2024.

Nowell, L. S., Norris, J. M., White, D. E., & Moules, N. J. (2017). Thematic analysis: Striving to meet the trustworthiness criteria. *International journal of qualitative methods*, 16(1), 1609406917733847.

OECD. 2022. Financing SMEs and Entrepreneurs. Available at: <https://www.oecd-ilibrary.org/sites/4bada6a3en/index.html?itemId=/content/component/4bada6a3-en> Date of access: 21 March 2024.

OFM (n.d.). *OFM - The Sound of your life*. [online] OFM. Available at: <https://www.ofm.co.za/Content/8/frequencies> Date of access: 13 June. 2024.

Orb, A., Eisenhauer, L. & Wynaden, D. 2001. Ethics in qualitative research. *Journal of Nursing Scholarship*, 33(1): 93 – 96.

Patel, A. & Singh, R. 2020. Mapping the Regulatory Landscape of Digital Trade. *International Journal of Digital Law*, 9(1):55–70.

Pavlou, P.A. 2020. Understanding the role of perceived fairness in online trust. *Decision Sciences*, 51(1):120-140.

POPIA. 2013. Protection of Personal Information Act, No. 4 of 2013, Government Gazette, Republic of South Africa, 26 (3967). Available at: <https://www.gov.za/documents/protection-personal-information-act> Date of access: 23 Nov. 2023.

Price Waterhouse Coopers. 2008. Managing the information security workforce: A priority for business and government. Available at: <https://www.pwc.com/mt/en/publications/technology/smes-in-the-world-of-cyber.html> Date of access: 28 Nov. 2023.

Puhakainen, P. & Siponen, M. 2017. Improving employees' compliance through information systems security training: An action research study. *MIS Quarterly*, 41(4):107-125.

Quinlan, C. 2011. Business research methods. *South-Western Cengage Learning*. 289.

Ramokgadi, T. & Katuu, S. 2021. The role of government in enhancing information security in the public and private sectors in South Africa. *Records Management Journal*, 31(1):74-90.

Republic of South Africa. 2013. Protection of Personal Information Act (POPIA), Act No. 4 of 2013. Pretoria: Government Printer.

Resnik, D.B. 2020. What is ethics in research and why is it important? National Institute of Environmental Health Sciences.

Rogers, E.M. 2003. *Diffusion of Innovations*. 5th ed. New York: Free Press. p. 221.

Rogers, R.W. 1975. A protection motivation theory of fear appeals and attitude change. *Journal of Psychology*, 91(1):93-114.

Rogers, R.W., 1975. *A protection motivation theory of fear appeals and attitude change*. *Journal of Psychology*, 91(1), pp.93–114.

Romanosky, S. 2016. Examining the costs and causes of cyber incidents. *Journal of Cybersecurity*, 2(2):108-121.

Rubin, H. J. & Rubin, I. S. 2005. *Qualitative interviewing: The art of hearing data*. Thousand Oaks, CA: Sage.

Safa, N.S., Von Solms, R. & Furnell, S. 2016. Information security policy compliance model in organizations. *Computers & Security*, 56:409-425.

Saunders, M., Lewis, P. & Thornhill, A. 2007. Research Methods for Business Students. Upper Saddle River, NJ: Pearson.

Saunders, M., Lewis, P. & Thornhill, A. 2012. *Research Methods for Business Students*. Harlow: Pearson Education.

Saunders, M., Lewis, P. & Thornhill, A. 2015. *Research Methods for Business Students*. Harlow: Pearson.

Saunders, M., Lewis, P. & Thornhill, A. 2016. *Research Methods for Business Students*. 7th ed. Harlow: Pearson.

Scholtz, B., Hughes, L., Sims, J. & Workman, M. 2020. Social engineering threats and information security risk management. *Computers & Security*, 89:86-95.

Scholtz, B., Kapeso, M. and Calitz, A., 2020. *Cybersecurity awareness campaigns for South African small businesses*. In: Proceedings of the 5th International Conference on the Internet, Cyber Security and Information Systems (ICICIS). [online] pp.1–9.

Singh, A. & Van Belle, J.P. 2020. Factors influencing the adoption of information security best practices in South African SMEs. *South African Computer Journal*, 32(1):91-100.

Siponen, M. & Vance, A. 2018. Neutralization: New insights into the reasons for IS security policy violations. *MIS Quarterly*, 44(1):87-106.

Siponen, M. & Vance, A., 2018. Guidelines for improving the contextual relevance of field surveys: The case of information security policy violations. *European Journal of Information Systems*, 27(2), pp.129–150.

Smith, J. & Johnson, L. 2016. Digital interactions: Exploring customer behaviour in online domains. *Journal of Internet Commerce*, 15(2):148–166.

Smith, J. & Johnson, L. 2022. *Fundamentals of Research Methods*. 2nd ed. Pretoria: Pretoria University Press.

Smith, J. 2014. *Online Privacy and Security: A global overview*. New York: Tech Press.

Smith, J. 2018a. Building Trust in Online Business Platforms: A user-centric approach. *Journal of Business Ethics*, 40(3):25-37.

Smith, J. 2018b. Ensuring data accuracy in qualitative research: An exploration of transcription quality. *International Journal of Qualitative Methods*, 17(1):160940691876328.

Smith, J. 2019a. Digital Trust and Commerce: A Global Perspective. Oxford: Oxford Business Press.

Smith, J. 2019b. Online Platforms and Market Dynamics in Central South Africa. Pretoria: South African Digital Publishers.

Smith, J., Thompson, A. & Roberts, K. 2019. A Guide to Research Approaches. Elmwood Press.

Smith, J., Thompson, A. & Roberts, K. 2022. Navigating Research Pathways. Elmwood Press.

Smith, J.P. & Lange, L.M. 2016. Effective online communication strategies for small businesses in South Africa. *Journal of Business Communication*, 33(2):112–130.

South African Cities Network. 2016. Sasolburg Economic Profile. Retrieved from <https://www.sacities.net/sasolburg>. Date of access: 19 June 2024.

South African Cities Network. 2018. Klerksdorp Economic Analysis. Retrieved from <https://www.sacities.net/klerksdorp>. Date of access: 19 June 2024.

South African Department of Trade and Industry. 2021. Digital Transformation and SME Growth.

South African Government. 2020. Government interventions for small businesses during the COVID-19 pandemic.

Southern African Venture Capital and Private Equity Association. 2021. Venture Capital Industry Survey.

Statistics South Africa. 2020. Municipal Demarcation and Economic Data. Retrieved from <http://www.statssa.gov.za/publications>. Date of access: 19 June 2024.

Statistics South Africa. 2021. Statistics of liquidations and insolvencies (Preliminary) May 2021. Available at: <http://www.statssa.gov.za/publications/P0043/P0043May2021.pdf>. Date of access: 05 Oct. 2023.

Steel, R. 2001. Internet Adoption in South Africa: Trends and Implications. *South African Journal of Business Management*, 32(2):45–58.

Tikkinen-Piri, C., Rohunen, A. & Markkula, J. 2018. EU general data protection regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review*, 34(1):134-150.

Tsai, J.Y., Egelman, S., Cranor, L.F. & Acquisti, A. 2017. The impact of privacy awareness on privacy-related behavior. *Journal of Human-Computer Interaction*, 32(8):603-623.

Van der Merwe, A., Van der Walt, J. & Van Rensburg, L. 2019. Digital Markets and Consumer Behaviour in South Africa. Pretoria: SA Publishers: 45.

Van der Merwe, R. & Pretorius, L. 2017. Small business online visibility in South Africa: A case study. *Journal of Business & Retail Management Research*, 11(3): 210 – 218.

Van Niekerk, J., Von Solms, R. & Labuschagne, L. 2005. An Information Security Governance Framework. *Information Management & Computer Security*, 13(4): 296 – 304.

Venkatesh, V. & Davis, F.D. 2000. A theoretical extension of the technology acceptance model: Four longitudinal field studies. *Management Science*, 46(2):186-204.

Venkatesh, V., Thong, J.Y. & Xu, X. 2012. Consumer acceptance and use of information technology: Extending the unified theory of acceptance and use of technology. *MIS Quarterly*, 36(1):157-178.

Venkatesh, V., Thong, J.Y.L. and Xu, X., 2012. *Consumer acceptance and use of information technology: Extending the unified theory of acceptance and use of technology*. *MIS Quarterly*, 36(1), pp.157–178.

Verizon. 2020. 2020 Data Breach Investigations Report. (online) Available at: <https://www.verizon.com/business/resources/reports/dbir/>.

Von Solms, R. and Van Niekerk, J., 2013. From information security to cybersecurity. *Computers & Security*, 38, pp.97–102.

Walker, E. 2018. *Regulations and Online Privacy in South Africa*. Durban: South African Regulatory Board Publications.

Xue, M., Nam, K. & Shen, R. 2020. Consequences of privacy policy on user trust on online platforms. *Journal of Information Privacy and Security*, 16(2): 123 – 137.

Yoon, C. 2019. Extending the theory of planned behavior in the context of information security compliance behaviour. *Computers & Security*, 87:72-84.

ANNEXURE A: INFORMED CONSENT LETTER

INFORMED CONSENT FORM

Purpose of the study:

You are invited to participate in a research study titled "Examining Factors Influencing Business Perceptions of Online Privacy and Security Risk in Central South Africa." The study's purpose is to understand how medium-sized enterprises perceive risks to online privacy and security and how these perceptions influence their business decisions.

What you will be asked to do:

If you agree to participate in the study, you will be asked to participate in an online or telephone interview of 30 to 45 minutes. During the interview, you will be asked to share your experiences, thoughts, and strategies related to the privacy and security of online transactions in your business.

Confidentiality:

Your answers remain confidential. Any information identifying you or your business will be removed before the data is analyzed. The data are securely stored, and only researchers (Xolani Boqo) and research supervisors can access them. The interview recordings are destroyed after the study has ended.

Voluntary participation:

Participation in this study is entirely voluntary. You can withdraw at any time during the study without penalty or consequence.

Benefits and Risks:

- Benefits: Although you will not benefit directly from participating, your contributions will help better understand online privacy and security issues in Central South Africa. This could help inform future business practices.
- Risks: The risks associated with participation are minimal. You can choose to skip any questions that make you uncomfortable.

Contact Information:

- Researcher: Mr. Xolani Boqo
Email: xolani.boqo@nwu.ac.za
Phone: +27 78 641 7382 or +27 79 666 2615
- Supervisor: Mr. Johannes Coetzee
Email: Johannes.coetzee@nwu.ac.za

By signing below, you indicate that you have read and understood the information and agree to participate in this research study.

Participant's name: _____

Participant's signature: _____

Date: _____

ANNEXURE B: LETTER OF GOODWILL

GOODWILL FORM

Subject: Permission for Research Study within **xxxx xxxx xxxx**

Dear NWU Business School,

We, XXXXXX, grant permission to Xolani Boqo, a student at North-West University, to conduct a research study within our organisation as part of their academic requirements. The study, titled **“Examining Factors Influencing Business Perceptions of Online Privacy and Security Risk in Central South Africa,”** aims to explore business perspectives on online privacy and security concerns and will contribute to the field of research in this area.

The study will be conducted in a manner that ensures minimal disruption to our daily operations. Xolani Boqo has assured us that all data collected will be handled confidentially and used solely for academic purposes. Furthermore, participation in the study will be voluntary for our employees, and appropriate ethical considerations will be followed in accordance with university guidelines.

Should you require any additional information regarding this permission, please do not hesitate to contact us at +27 xx xxx xxxx or email us at xxxxxx@xxxx

We appreciate the opportunity to support academic research and look forward to contributing to the success of this study.

Sincerely,

xxxxxx

Manager/Owner

xxxxxx

X

Company stamp/Signature

ANNEXURE C: PERMISSION TO CONDUCT INTERVIEWS LETTER

PERMISSION TO CONDUCT AN INTERVIEW

Xolani Boqo
MBA Student
079 666 2615
xolani.boqo@nwu.ac.za

XXXXX XXXXX XXXXX
XXXXX XXXXX street
XXXXXXXXXX

Dear XXXXX XXXXX

I hope this letter finds you well. My name is Xolani Boqo, and I am currently conducting a research study titled "Examination of Factors Influencing the Perception of Corporate Online Privacy and Security Risks in Central South Africa" as part of my Master of Business Administration (MBA) programme at the North-West University Potchefstroom Campus.

The study aims to understand how South African companies perceive and manage the risks associated with online privacy and security. The study aims to provide valuable insights that can help enhance digital trust and security practices among local companies.

I am writing to request your permission to conduct an interview with you or a designated representative of your business. The interview will cover topics such as your business experience and practices in online privacy and security. It will take 30-45 minutes and can be held at a convenient time for you, including by phone, email, or online meeting platform.

Participation in this study is completely voluntary, and you can choose to withdraw at any time without consequences. All information collected during the interview will be kept strictly confidential and used only for academic purposes. The identification of business and personal information details is anonymous to ensure privacy.

If you agree to participate, please sign the attached consent form and email it to me at xolani.boqo@nwu.ac.za or send a WhatsApp message to +27 79 666 2615.

Thank you for considering my request. Your participation is appreciated and will make a significant contribution to the success of the research. If you have any questions or need more information, please contact me at: +27 79 666 2615 or xolani.boqo@nwu.ac.za

I look forward to hearing your positive response.

Sincerely,
Xolani Boqo MBA Student
North-West University
+27 79 666 2615

ANNEXURE D: DATA COLLECTION TOOL

Semi-Structured Interview Guide

Introduction:

Good day and thank you for agreeing to meet with me today.

My name is Xolani Boqo, and I am a student at North-West University, pursuing my MBA. I am conducting research under my mini-dissertation, which entails examining the factors influencing business perceptions of online privacy and security risks in Central South Africa. Your background as a business manager/owner makes you highly relevant for this study.

The interview will take only about 30 to 45 minutes of your time.

With your permission, I would like to audio record our conversation to ensure that I accurately capture your responses. Do not fear; all that you say will be kept confidential. Your identity will be anonymised in all the reports, and the information you provide will only be used for academic purposes.

Responding to this interview is entirely voluntary. You can choose to decline to answer any or all of the questions or withdraw at any time without penalty.

Before continuing, may I respectfully confirm that you are willing to participate and consent to being recorded?

INTERVIEW QUESTIONS:

Section 1: Background Information

1. Could you briefly describe your role in the company?
2. How long have you been in the industry?

3. What are the primary online platforms or tools your business relies on for operations?

Section 2: Perceptions Of Online Privacy Risks

4. What concerns do you have regarding online privacy in your business?
5. How do this privacy concerns impact your day-to-day operations?

Section 3: Perceptions of Online Security Risks

6. How would you describe the online security risks your business faces?
7. What measures have you implemented to mitigate these risks?

Section 4: Managerial Knowledge and Awareness

8. Can you describe your level of knowledge or training on digital privacy and cybersecurity principles?
9. Do you believe your team or business is well-informed about these topics?

Section 5: Impact on Business Decisions

10. How do concerns about privacy and security influence your business decisions?
11. Can you give an example of a business decision influenced by these concerns?

Section 6: Trust in Online Platforms

12. How much trust do you place in the online platforms you use?
13. What factors contribute to or reduce your trust in these platforms?

Section 7: Cultural and Contextual Influences

14. Do you think cultural or political factors in your region influence how your business views online privacy and security?
15. Can you share any examples of how these factors might affect your approach or decisions?

Section 8: Experiences with Privacy or Security Breaches

16. Have you experienced any breaches related to online privacy or security?

17. What was the impact of this breach, and how did your business respond?

Section 9: Recommendations and Sentiments

18. What do you think SMEs in your region need to improve their online privacy and security?

19. Are there any tools, training, or support systems you believe would help?

Conclusion:

Thank you once again for taking the time to participate in this study. Your insights and experiences are truly valuable and will make a meaningful contribution to the research findings.

If you have any final thoughts or additional comments you'd like to share, please feel free to do so; your input is always welcome.

Should you be interested, I would be happy to share a summary of the final results once the study is complete

If you have any questions or would like to follow up at any time, please don't hesitate to

Contact me at:

Email: xolani.boqo@nwu.ac.za

Phone/WhatsApp: +27 79 666 2615

Thank you once again for your support and contribution.

ANNEXURE E: ETHICS APPROVAL LETTER

ETHICS APPROVAL LETTER



Private Bag X1290, Potchefstroom
South Africa 2520

Tel: 018 299-1111/2222

Fax: 018 299-4910

Web: <http://www.nwu.ac.za>

Senate Committee for Research Ethics

Tel: 018 299-484

Fazwa.Miseleni@nwu.ac.za

03 September 2024

ETHICS APPROVAL LETTER OF STUDY

Based on approval by the **Economic and Management Sciences Research Ethics Committee (EMS-REC)** on, **03/09/2024** the Economic and Management Sciences Research Ethics Committee hereby **approves** your study as indicated below. This implies that the North-West University Senate Committee for Research Ethics (NWU-REC) grants its permission that, provided the special conditions specified below are met and pending any other authorisation that may be necessary, the study may be initiated, using the ethics number below.

Study title: Examining factors influencing business perceptions of online privacy and security risk in Central South Africa									
Study Leader/Supervisor (Principal Investigator)/Researcher: Mr. J.C. Coetzee									
Student: X. Boqo (28744780)									
N	W	U	-	0	1	7	3	7	-
Institution		Study Number			Year		Status		
Status: S = Submission; R = Re-Submission; P = Provisional Authorisation; A = Authorisation									
Application Type:									
Commencement date: 03/09/2024					Risk: Minimal				
Expiry date: 03/09/2025									
Approval of the study is initially provided for a year, after which continuation of the study is dependent on receipt and review of the annual (or as otherwise stipulated) monitoring report and the concomitant issuing of a letter of continuation.									

Special in process conditions of the research for approval (if applicable):

- None.

General conditions:

While this ethics approval is subject to all declarations, undertakings and agreements incorporated and signed in the application form, the following general terms and conditions will apply:

- The study leader/supervisor (principle investigator)/researcher must report in the prescribed format to the EMS-REC:
 - annually (or as otherwise requested) on the monitoring of the study, whereby a letter of continuation will be provided, and upon completion of the study; and
 - without any delay in case of any adverse event or incident (or any matter that interrupts sound ethical principles) during the course of the study.

ANNEXURE F: LANGUAGE EDITING CERTIFICATE



Centre for Scholarly Publishing Services (PTY) Ltd

Reg no: 2015/44302/07

11 August 2025

TO WHOM IT MAY CONCERN

XOLANI BOQO

Noth West Business School
Faculty of Economic and Management Sciences
North West University Business Schools
Potchefstroom, South Africa

This serves to confirm that an MBA mini-dissertation titled *Examining factors influencing business perceptions of online privacy and security risk in central South Africa* by Xolani Boqo and submitted in partial fulfilment for the degree Master of Business Administration (MBA) at the North-West University Business School has undergone both a thorough copy-editing as well as proof-reading processes.

Sincerely,



With best wishes,

Solani Ngobeni
Publishing Director

Centre for Scholarly Publishing Services (Pty) Ltd
Cell: [+27 61 506 6115](tel:+27615066115)

solani@cspss.co.za www.cspss.co.za