

Investigating involvement of leaders in technology discussions as mitigating factors of cyber risk in SMEs

R Pretorius



orcid.org/0000-0002-9806-9967

Mini-dissertation accepted in partial fulfilment of the
requirements for the degree [Master of Business
Administration](#) at the North-West University

Supervisor: Dr N Ndlovu

Graduation: June 2023

Student number: 23345675

PREFACE

Réno Pretorius, the researcher in this study, has worked in the IT industry for 27 years. He started as an IT technician in the financial services industry and was quickly promoted to senior technician. He then headed the software quality assurance department and was later appointed as the IT operations manager. He also worked as a customer and third-party liaison, coordinating with the various banks in South Africa and the Reserve Bank for system and functionality testing and ensuring daily processing operations were running effectively. After nine years, he decided to join a friend in a web development company for a year and a half and then started a new IT business. The 12-year-old business now provides IT and business consulting services combined with total IT solutions from network cabling, VOIP, and IT support services to cloud servers for SME businesses. Website and domain hosting and development services are also performed. The researcher thus has extensive experience in the IT industry and within various IT sectors to provide relevant IT consulting services to businesses. Reno has completed Business Management, Management Consultancy, and Management Strategy courses and a post-graduate diploma in management at the NWU Business School. An MBA was the logical next step to properly prepare for the changes surrounding the fourth industrial revolution and combine IT and business consulting to enhance the quality and efficiency of consulting to SME business customers. The next step is to register as a business consultant and start an organisation to help other young entrepreneurs grow their businesses and help them navigate the pitfalls. Additionally, the business provides not-for-profit services to other NPOs and education institutions to assist them in growing and improving the country.

This study started from an observation that SME leaders are not always involved or present in IT discussions and are uninformed or misinformed through second-hand discussions. The results are that businesses are at risk of being compromised, losing data or being fined for illegal licensing, which could all be prevented if the leader attended a few sessions. Additionally, they are unaware of the potential benefits and competitive advantages that technology can provide while mitigating these risk factors. This study was challenging but provided some interesting insights and perceptions from SMEs regarding technology and involvement.

ACKNOWLEDGEMENTS

First and foremost, I would like to use this opportunity to thank my heavenly Father and saviour for the opportunity and for helping me cope. Secondly, I want to thank my family for supporting me, especially my wife, for being very supportive, and without her, I would not have been able to manage and complete the course. Similarly, a big thanks to the employees and colleagues at the Entrutech for maintaining order and a high level of customer service while also supporting me through the journey.

I would also like to thank the NWU Business School and all the lecturers for the guidance and knowledge transfer that is truly invaluable.

ABSTRACT

Problem: The lack of involvement and participation by primary decision-makers increases the risk to the business.

Objective: This study investigates the significance of the relationship between leadership involvement in technology discussion and the perceived technology risks to the business.

Methods: This quasi-experimental study utilised a closed-ended, structured questionnaire with a 7-point Likert scale to obtain primary data before and after information sessions (manipulation) to determine the change in the level of involvement (independent variable) and the risk perception (dependent variable).

Findings: The results indicate significant correlations in the relationship between leadership and the leader's perceived risk to the business, which is consistent with the study's primary objective.

Discussion: Increased awareness of the importance of information technology and its implication on the business will likely also increase the risk perception of respondents, at least increasing the demand for cybersecurity training and preventative and mitigation options like obtaining insurance against cybercrime. Being involved and thus more aware of the impact of information technology in the business will help leaders make better-informed decisions to help businesses succeed and understand the risks to the business.

Keywords: Technology involvement, risk perception, SME Cyber risk, cybercrime, risk management, risk mitigation, technology adoption, competitive advantage.

TABLE OF CONTENTS

PREFACE	I
ACKNOWLEDGEMENTS.....	II
ABSTRACT	III
TABLE OF CONTENTS.....	IV
LIST OF TABLES	VIII
LIST OF FIGURES.....	IX
DEFINITION OF TERMS	1
LIST OF ABBREVIATIONS	3
CHAPTER 1: NATURE AND SCOPE OF THE STUDY	4
1.1 Introduction and background.....	4
1.2 Problem statement	5
1.3 Research objectives.....	5
1.3.1 Primary objective	6
1.3.2 Hypotheses.....	6
1.4 Scope of the study and delimitations.....	6
1.4.1 Field of study	6
1.4.2 Businesses under investigation	6
1.5 Ethical considerations	7
1.6 Contribution of the study	7
1.7 Limitations of the study	7
1.8 Chapter summary.....	8
CHAPTER 2: LITERATURE REVIEW	9
2.1 Overview and introduction.....	9
2.2 Awareness	9

2.3	Risk	10
2.4	Risk responsibility	11
2.5	Risk management	12
2.6	Risk factors in SME	13
2.7	Technology in SME, risk or opportunity?	13
2.8	Technology success factors in business	15
2.9	People, culture, and leaders.....	16
2.10	Quality of information and processes	17
2.11	Competitive advantage	18
2.12	Conceptual framework	19
2.13	The gap in evidence (The missing piece in related cases).....	20
2.14	Chapter summary.....	20

CHAPTER 3: RESEARCH DESIGN AND METHODS 22

3.1	Chapter introduction.....	22
3.2	Research philosophy and paradigm.....	22
3.3	Research strategy	23
3.4	Research choices.....	23
3.5	Technique and procedure	23
3.6	Study population and sampling	23
3.6.1	Defining the population.....	23
3.6.2	Sample	24
3.6.3	Sample size	24
3.6.4	Inclusion criteria.....	25
3.6.5	Exclusion criteria	25
3.6.6	Sample limitations or errors.....	25
3.7	Relationship between the researcher and the participants.....	25

3.8	Recruitment of potential respondents.....	26
3.9	Measuring instruments and data collection	26
3.10	Reliability and validity	27
3.11	Data and statistical analysis	27
3.12	Ethical issues and informed consent.....	28
3.13	Other ethical considerations.....	29
3.14	Chapter summary.....	30
CHAPTER 4: DATA ANALYSIS AND DISCUSSION OF FINDINGS.....		31
4.1	Chapter introduction (review)	31
4.2	Demographics and background	31
4.3	Frequencies and descriptive statistics.....	34
4.3.1	Involvement	34
4.3.2	Risk.....	36
4.4	T-tests, Wilcoxon and Mann-Whitney tests	37
4.4.1	Dependent t-test and Wilcoxon test	37
4.4.2	Result: IT tools and security as a waste of money.....	38
4.4.3	Result: Cyber disaster likelihood	39
4.4.4	Result: Cybersecurity training	40
4.5	Independent t-test and Mann-Whitney U Test.....	40
4.5.1	Result: Previous cyber-attack against the likelihood of happening	41
4.5.2	Result: Delegate tendency depending on the position.....	41
4.6	Correlations.....	42
4.6.1	Result: Awareness.....	42
4.6.2	Result: Awareness.....	43
4.6.3	Result: Technical understanding	44
4.6.4	Result: Technical understanding	44
4.7	Discussion.....	45

4.8	Hypothesis results.....	46
4.8.1	H1 result	46
4.8.2	H2 Results	47
4.8.3	H3 Results	47
4.8.4	H0 Results	48
4.9	Chapter conclusion	48
CHAPTER 5: IMPLICATIONS AND LIMITATIONS.....		49
5.1	Chapter introduction.....	49
5.2	Research questions and resolutions	49
5.3	Implications	50
5.3.1	Involvement or participation	50
5.3.2	Awareness.....	50
5.3.3	Culture	50
5.4	Recommendations	51
5.5	Limitations.....	51
5.6	Future research.....	51
REFERENCES.....		52
ADDENDUM A: ETHICAL CLEARANCE.....		57
ADDENDUM B: QUESTIONNAIRES, CONSENT FORMS AND INFORMATION SESSION		58
ADDENDUM C: LANGUAGE EDITOR CERTIFICATE		67
ADDENDUM D: SIMILARITY INDEX		68
ADDENDUM E: DESCRIPTIVE STATISTICS		69

LIST OF TABLES

Table 1: Involvement Frequency statistics summary	35
Table 2: It tools and security as a waste of money	38
Table 3: Cyber disaster likelihood	39
Table 4: Cybersecurity training	40
Table 5: Test results for previous cyber-attack experiences and likelihood	41
Table 6: Delegate tendency independent T-test, depending on the position	42

LIST OF FIGURES

Figure 1: Impact of decision-maker (DM) traits on company technology adoption	17
Figure 2: Conceptual framework	20
Figure 3: Position at company	32
Figure 4: Level of education	32
Figure 5: Primary decision-maker	33
Figure 6: Previous cyber attacks experienced.....	33
Figure 7: Security policy in place.....	34

DEFINITION OF TERMS

Leaders

The owners, leaders, C-level executives and primary decision makers or management of a business, who have the final say in implementing technology in the organisation.

SMEs

The South African Department of Small Business Development defines SMEs as small and medium enterprises with fewer than 250 employees and, depending on the industry, generally less than R 220 million in total annual revenue (Department of small business development, 2019:111).

Technology

Any technology utilised in business to improve business operations, security, or decision-making.

Digital transformation

The implementation and adoption of technology in an organisation to improve business processes and operations and further effect change in the culture to utilise these technologies efficiently.

Competitive advantage

An organisation's factors or attributes that distinguish it from its competitors, thus allowing for better performance.

Involvement

A person being present in meetings, actively participating and collaborating, caring about the topic and wanting to know more.

Knowledge management

The actions taken by an organisation to collect and create institutional knowledge and the methods to share, use and manage the knowledge databases and ensure its security.

Cyberattacks

Internet criminal activity aiming to cause damage, destroy, or obtain information about an organisation. Additionally, using the information for ransom purposes or causing further reputational damage.

Risk Management

Risk management is defined by ISO (2018) as an organisation's coordinated activities to direct and control risk.

LIST OF ABBREVIATIONS

ISO	The international organisation for standardisation
IT	Information technology
NIST	The National Institute of Standards and Technology
SME	Small and medium enterprise

CHAPTER 1: NATURE AND SCOPE OF THE STUDY

1.1 Introduction and background

To handle the changing technology and business environments, organisations should incorporate technology into business risk management and understand the role in overall business and risk management (Marx & Schutte, 2018:61). Business leaders can no longer ponder whether they should digitalise or not, as Schreckling and Steiger (2017:23) highlight that it is imperative and can be detrimental to a business. However, frameworks and models are available to guide SMEs with their digitalisation journey (Georgiadou, Mouzakitis, Bounas & Askounis, 2020:9; Jere & Ngidi, 2020:7; Nel & Drevin, 2019:161; Schreckling & Steiger, 2017:19). But, to understand and utilise these models and frameworks, and implement them with success, business leaders must be involved in all technical discussions to understand these digitalisation potentials and associated risks better.

As a technology consultant, the researcher encountered the problem that the primary decision-makers are not always involved in technology discussions but instead delegate tasks to others. The results are that they make uninformed critical decisions about systems and core security that greatly influence their business strategy and success and open the business to undue risks. Much information exists in the news and internet about cybercrime statistics and the resultant costs and risks (Keeper, 2021:4-6). However, there are far fewer in the context of these risks due to neglected leadership involvement.

This study investigates the relationship between the decision maker's involvement in technical discussions and their perception of risks to the business. With the results, the researcher strives to create awareness with business leaders to realise the importance of their involvement in every technology function, as they do with finances and other strategic business functions. They must not see it as just another expense item on the financial statements.

The study will follow a quantitative experimental design to test the relationship between the decision maker's involvement (independent variable) and the perceived risks to the business (the dependent variable). Primary data will be collected with questionnaires before and after an intervention session. Data will be analysed with descriptive and relational statistics using IBM SPSS (Version 25.0) software to determine the relationships.

1.2 Problem statement

Technology has changed how we do business. It defines business processes, efficiencies and overall competitive advantage. It is at the core of any business today (Schreckling & Steiger, 2017:23). Yet, the disconnect between a leader's technology readiness traits and perception of technology cause unnecessary risks to the business (Reynolds, Cotrino, Ifedi & Donthu, 2020:11-12).

With the move to remote work resulting from Covid 19 lockdowns, there is a growing reliance on technology infrastructure to remain sustainable and competitive (CSO:1). The CSO (2021:7) report highlights that 71% of respondents mentioned that their security budget would increase to mitigate these risks. 79% Noted that the impact of such attacks is critical or catastrophic; however, it further highlights that the people factor in terms of awareness is still lagging. Unfortunately, organisations and their leaders only implement the required changes after experiencing severe damage from cyber attacks. Keeper (2021:4) noted in a study of 2000 employees that the required change only happens after such losses, with 87% of organisations implementing stricter security, 90% providing employees with additional cybersecurity training, and 67% increasing their spending towards technology security.

Schreckling and Steiger (2017:3) highlight the importance in their statement that *"digitisation is no longer a choice but an imperative"*.

However, the problem experienced in SMEs is the limited involvement of decision-makers in technology discussions, causing a skewed perception and limited awareness of real risks to the business. In turn, this disconnect limits the adoption and integration of technology into business strategy, directly impacting the business risks and limiting the potential success or competitive advantages the organisation could achieve with proper integration. Clearly, the primary decision-maker's lack of involvement and participation in technology discussions increases the risk to the business.

1.3 Research objectives

The objectives and supporting hypotheses will attempt to answer the following question: Does the level of leadership involvement in technology discussions impact a leader's perceived risk to the business?

1.3.1 Primary objective

The primary objective of this study is to determine the significance of the relationship between leadership involvement in technology discussion and the perceived internal and external technology risks to the business.

1.3.2 Hypotheses

The researcher deduces hypotheses from theory or practice, which must be subjected to empirical research (Bryman, Bell, Hirschsohn, dos Santos *et al.*, 2014:9). In support of the primary objective, this study will empirically research and test the relationship between the variables with these hypotheses:

H1: There is a positive relationship between decision-maker involvement in technology discussion and their perceived risk to the business.

H2: Increased technical understanding of the decision-maker positively correlates with the perceived risks of the business.

H3: There is a positive correlation between decision-maker involvement and technology adoption and integration into business strategy.

H0: There will be no difference in the respondent's perceived risk to the business after the information session.

1.4 Scope of the study and delimitations

1.4.1 Field of study

The field of study is general management. Technology should no longer be separated from management but should be a part of every strategic decision in every business function. Also, management should be involved in all technical discussions to ensure they are aware of all potential risks and opportunities from technology in their businesses.

1.4.2 Businesses under investigation

This study investigates small and medium-sized enterprises in the North West and Vaal triangle areas of South Africa, employing full-time employees that use computers daily.

The study focuses on businesses registered with these areas' respective chambers of commerce.

1.5 Ethical considerations

The researcher took great care to ensure high ethical standards throughout this study regarding interaction with participants, data collection, statistical analysis and presentation of information. The researcher followed the process below to ensure ethical standards throughout the study:

- The researcher contacted the Potchefstroom Chamber of Commerce chairman to obtain approval to present the study to their members and contacted members of The Golden Triangle Chamber of Commerce and the Matlosana Chamber to obtain approval to send the questionnaires to their members.
- The respective chambers of commerce sent the request to participate in the study through their communication channels, thus limiting direct interaction with the researcher.
- Participation was entirely voluntary, with a detailed description of the process they could expect.
- The information sessions were available to watch at any time, and no information was gathered from the participants while watching the presentations.

1.6 Contribution of the study

The study aims to contribute knowledge about leadership involvement's impact on business risks, opportunities and sustainability. The information session will enlighten decision-makers on their required involvement to improve awareness and understanding of these risks and help them make more informed decisions to mitigate them. It will further provide insight into how much a decision-maker's perspective on business risk might change when they attend discussions and information sessions.

1.7 Limitations of the study

The study sample focussed on SMEs registered with a chamber of commerce in the North West and Gauteng province. Hence it is not representative of all SMEs in these provinces or the greater South Africa. Due to the low response rate from the Potchefstroom

Chamber of Commerce, the researcher expanded the population scope of the study by including The Golden Triangle Chamber of Commerce and the Matlosana Chamber of commerce. After including these other chambers of commerce, the number of respondents was minimal (N=36), thus limiting the study's potential.

1.8 Chapter summary

This chapter started by introducing the background to the study and discussing the empirical problem. The research questions, objectives and related hypotheses that form the basis of this study were then explained. The scope, delimitations and ethical considerations set the study's boundaries to ensure high ethical standards and provide direction for the following chapters. Lastly, the contributions and limitations of the study concluded the chapter. The next chapter will elaborate further on the current literature regarding leadership involvement, awareness and risk perception of cyber risks in SMEs.

CHAPTER 2: LITERATURE REVIEW

2.1 Overview and introduction

The literature review aims to familiarise the reader with technological and risk concepts that impact the success of a business, as well as the importance of leadership involvement in making informed decisions related to these concepts. Moreover, it highlights the gap between the current literature and the problem identified. This chapter will elaborate on the risks associated with SMEs and the perception or behaviour of SME decision-makers and leaders towards technology. Awareness forms the foundation of this chapter, expanding into risks associated with cybercrime to SMEs, who the responsible persons are, and what risk mitigation entails. The rest of the chapter also explains how SMEs and their leaders can manage such risk by incorporating these discussions into strategic management processes and company culture.

2.2 Awareness

The drive for efficiency and automation in the world continues to drive exponential growth and an unprecedented demand for data, requiring constant technological innovation and leading to the creation of entirely new technologies (Hodson, 2019:6). Hodson (2019:5) further notes that companies are undergoing digital transformation because an information-centric world requires a shift in how companies are run and how they deliver projects and manage risk.

IT security and risk management are fundamentals of everything an organisation does, and awareness of cybersecurity and best practices should reach every line of business and every employee (Hodson, 2019:76; Scholtz, 2019:2). The lack of security awareness and the SME challenges differ only depending on the company size and market segment but are similar across countries (Hoppe, Gatzert & Gruner, 2021:254; Reynolds *et al.*, 2020:12; Schutte & Marx:17-18). Veiga, Looock and Renaud (2022) found that cyber awareness differs between developed and developing countries. The latter face distinct challenges regarding personal capabilities, needs, legislation and infrastructure availability. In developing countries, cyber training and measurements require a different approach altogether.

The CEO drives the core strategy but requires critical input from the CIO and CFO regarding budget, technology transformation and adoption. In smaller businesses, which

cannot afford a CIO, this poses a problem in the form of a gap in the security awareness of the business. As explained in the study by SAGE (2020:3), all C-level players need to be involved in business strategy in larger organisations. In reality, Saban, Rau and Wood (2021:278) concluded that the very career of an executive might be vulnerable if their organisation is adversely affected by a breach of information security. Moreover, an organisation's sustainability and success depend on the participation of management in cybersecurity discussions. However, many SMEs perceive themselves as too small or irrelevant for cybercriminals to target them, thus creating an inadequate level of awareness.

As a result, SMEs fail to appreciate cyber threat risks and neglect to deploy efficient security measures (Alahmari & Duncan, 2020:3; Hoppe *et al.*, 2021:248). Saban *et al.* (2021:278) highlighted that many SME executives still believe their businesses are not at risk and are not sufficiently motivated to improve their security position. They suggest three primary mistaken beliefs in SMEs: 1) the business is too small and irrelevant, 2) the basic protections implemented are sufficient, and 3) executives can rely on IT staff and employees to understand and manage security threats to the business, effectively absolving them of the need to be involved. Therefore, digital transformation is no longer solely the responsibility of the CIO or, in the case of SMEs, the IT consultant or IT team SAGE (2020:3). These beliefs, lack of awareness or involvement and, in some instances, ignorance, bring undue risks to the business.

2.3 Risk

The International Organization for Standardization ISO (2018:3) defines risk as "the effect of uncertainty on objectives". They stipulate that an effect is seen as a deviation from the expected outcome and can be positive, negative or both. Additionally, the effect can address, create or result in opportunities or threats. Moreover, Gartner identified supply chain attacks as a noteworthy domain gaining more attention from hackers, providing a gateway into larger companies through the supply chain (Firstbrook, Olyaei, Shoard, Thielemann *et al.*, 2022:2-4; Saban *et al.*, 2021:278). Increased use of digital systems, new hybrid working environments and public cloud solutions further escalate these risks. Information security influences the immediate business and the larger economy (PricewaterhouseCoopers, 2018:4). Supply chains are tightly integrated into digital and operational systems, increasing the vulnerability and potential for attacks. Thus, supply

chain attacks will expose businesses to liability if they do not comply with basic security principles or regulations. Clearly, cybersecurity is not just about the organisation's own business anymore. It impacts the entire supply chain.

However, this study focuses more on cyber risk. Eling and Schnell (2016:483) derived the following definition of cyber risk for the insurance industry after consolidating 209 papers on cyber risk:

"Any risk emerging from the use of IT that compromises the confidentiality, availability or integrity of data or services."

Interestingly, the World Economic Forum global risks report mentions digital inequality and failure to manage cybersecurity as blind spots that can lead to top business risks in the next two to three years (WEF, 2022:23). Unfortunately, SMEs do not realise that damages due to cyber-attacks are not confined to monetary losses alone but also include downtime, data loss and even the loss of lives, as found by Al-rimy, Maarof and Shaid (2018:162).

2.4 Risk responsibility

Importantly, digital strategy is the cornerstone of a company's digital transformation (Hodson, 2019:6). However, going digital is not just implementing the greatest and latest technologies because others are doing it, but a method of achieving business goals. Hodson (2019:6) further highlight that requirements such as lowering costs, improving performance, or improving customer satisfaction should drive digital transformations. Additionally, digital strategy involves an investigation of the current IT assets and environment, continuous system improvement thorough relevant IT spending, and creating a plan to ensure the improvements positively influence the business goals.

Technology risk management should be an ongoing business issue, not a once-off technical project or delegated to another department (Hoppe *et al.*, 2021:254). SAGE (2020:3) states that Digital transformation and related risks are not uniquely the IT department's responsibility anymore but that of all management functions. They should be aware of the requirements, regulations and related risks if not adhered to. Saban *et al.* (2021:278) note that using technology information requires a holistic approach to the interaction between people, processes and technology.

Hammarberg and Gazzawi (2022:26-33) highlighted that effective leadership significantly influences the success of Information Security Risk Management (ISRM). Also, SMEs discuss risks and risk management informally but do not formally document the processes. Further, critical risks differ significantly between different organisations or industries. Due to these challenges, SME management tends to pick security priorities depending on their knowledge, experience and available resources, thus potentially exposing the organisation to unplanned and unknown risks. SAGE (2020:5) further highlights that managing fraud and cybersecurity risks is one of the primary challenges for financial professionals in South Africa.

Hodson (2019:xiv) note that it has been mentioned many times in the news that cybersecurity is a mainstream business function. He further notes, "*Cybersecurity is more than a nice to have for modern businesses.*" Technology integrates into every business function; therefore, strategic exercises should involve the entire management team, as reported by McKinsey, a global management consulting firm (Bughin, Catlin, Hirt & Willmott, 2018:15). Lewis and Kaiser (2019:10) highlight that IT should play an essential role in formulating business strategies. Firstbrook *et al.* (2022:17) corroborate this integration in their Gartner research that business leaders should manage and integrate cybersecurity as part of business technology and risk management instead of seeing it as a specialised IT role. They further state that businesses can only achieve benefits and thrive with cybersecurity in a hostile environment if they increase responsibility and accountability at the highest levels. IT teams can also make mistakes through misconfiguration or be unaware of security gaps. They are often unaware of the more comprehensive business strategy (Hodson, 2019:76). Therefore, management is responsible for being aware of the IT team's services and insisting on proper feedback and testing of all solutions.

2.5 Risk management

ISO (2018:3) note that the core purpose of risk management is to create and protect value in the organisation. All organisations face and should manage risks related to internal and external uncertainties which determine the success of business objectives, including human cultural factors and behaviour. Risk management is a repetitive process of coordinated activities organisations utilise to set strategies, improve performance, encourage innovation, achieve objectives and make informed decisions. Additionally, it

forms part of the governance, leadership and all activities associated with an organisation, including its stakeholders. These aspects are the fundamentals of managing organisations at all levels, resulting in improved systems and processes (ISO, 2018:1-3). With a risk management strategy, SMEs can improve the company in terms of legal status, capital, size and age. They are generally better prepared to handle cyber risks and achieve business objectives while improving their reputation and reducing risks (Hammarberg & Gazzawi, 2022:10).

2.6 Risk factors in SME

SMEs depend on technologies and networks for operations and decision-making processes. However, this dependency makes them vulnerable to technology security threats because they have limited financial, technical and skilled human resources to manage and prevent such threats (Moufida, Steven & Peter, 2020:468). According to Hammarberg and Gazzawi (2022:29), SMEs have inexperienced management that handles security and ISRM in a very informal manner. Moufida *et al.* (2020:470) further highlight that a critical challenge for most SMEs relates to integrating the security strategy into the business strategy and that the primary shortages are the lack of engagement to create security policies and not performing technology risk assessments. Additionally, due to the increasing demand for security specialists and skilled IT personnel, SMEs do not have the resources to obtain and retain highly sought-after skilled personnel (Hoppe *et al.*, 2021:253). Hammarberg and Gazzawi (2022:26) stress that regular ISRM frameworks and tools (like ISO 27001 and NIST SP 800-37) are designed for enterprises and not aligned with SMEs. They require resources and money, making them unaffordable for SMEs. Additionally, specific challenges for SMEs are the overconfidence effect, failed predictions of risk, limited knowledge sharing, and risk vs cost tradeoffs of leaders in SMEs (Hammarberg & Gazzawi, 2022:11).

2.7 Technology in SME, risk or opportunity?

Companies include technology management in their overall risk mitigation strategies, but the level of security implementation and risk awareness differ depending on the industry or market orientation (Reynolds *et al.*, 2020:12; Schutte & Marx:17-18). It is essential to instil a culture of proper security and knowledge management in every business function and ensure all departments focus on a security-first approach to all technology and

enhancement projects (de Koker & du Plessis, 2020:3). Importantly, Mukhopadhyay, Chatterjee, Bagchi, Kirs *et al.* (2019:1013) confirmed through the CRAM model that the probability of attack decreases with improved technology adoption. Nevertheless, Mukhopadhyay *et al.* (2019) note that several companies still view cyberattacks as "*the cost of doing business*" and that this attitude prevents them from taking a more proactive stance toward preventing attacks.

Information security should be a strategic priority in organisations that influence policies, procedures and, most importantly, the organisation's culture. All employees must understand the critical role information security plays in the organisation's success and sustainability (Saban *et al.*, 2021:278). Unfortunately, employee awareness of security risks is lagging (CSO, 2021:7). The human factor is still responsible for most data breaches, and current security awareness training is no longer practical (PricewaterhouseCoopers, 2018:4). Although cyber literacy and awareness are improving, traditional training only focuses on spotting cyber threats and does not address the latest trends. As a result, business and IT leaders do not make effective cybersecurity decisions (Firstbrook *et al.*, 2022:19). Hoppe *et al.* (2021:253) analysed 37 industry surveys and highlighted severe weaknesses in SME security culture as a significant challenge. These include risk perception, knowledge and the attitude of SME leaders and decision-makers towards cyber risk management. They also found a lack of know-how as an obstacle to risk awareness and identification of risks in SMEs.

Sharma and Aparicio (2022) established that organisation and team culture changes the employee's perception to evaluate cyber-risks, which changes their behaviour towards complying with security policies. To affect change in the security culture, the behaviour of all employees should change. However, raising awareness, changing behaviour, and therefore the risk perception of people in the organisation also depends very much on cultural differences (Bada, Sasse & Nurse, 2019:5). To change the behaviour, leaders and employees should understand the risks and apply the advice provided by IT and consultants. Additionally, they should be willing and motivated to change (Bada *et al.*, 2019:1). However, Bada *et al.* (2019:9) note that knowledge and awareness must also be implemented together with other business strategies to sufficiently change the behaviour of all employees and thus improve the organisational cyber security culture. Bada *et al.* (2019:2) highlight two primary reasons employees do not comply with expected behaviour or company policies. First, employees are unaware of the risks or do

not perceive the risk as a problem. Secondly, employees do not understand or know the reason for the expected behaviour. Therefore management must address cyber risk as a part of business strategy by improving the organisation's culture. They must start at the top and not just delegate responsibility (Hoppe *et al.*, 2021:254).

2.8 Technology success factors in business

Business and ICT strategy can no longer be separated. Every decision involves a balance of risk and reward and should integrate with all business functions as enablers of business performance and competitive advantage (Artemenko, 2020; Astuti, Suhadak, Rahayu & Wilopo, 2018:320,326; Marx, 2017:16-17; Reynolds *et al.*, 2020:11-12; Schutte & Marx:14; Sibanda & Ramrathan, 2017:198). Hoppe *et al.* (2021:243) Found that risk perception, knowledge and managerial attitude towards cyber risks are significantly lacking in the SME security culture. Gopal and Maweni (2019:87) concluded that organisations should continually gather and analyse information on their activities and processes to assess weaknesses in their security position with appropriate tools and techniques. Therefore, the decision-maker must be involved to understand them and incorporate these into the overall business strategy.

Technology changed how we do business. Leaders must consider various aspects of technology within their business strategy that will determine the success or failure of a business. Artemenko (2020:4); Astuti *et al.* (2018:326) stipulate that business information technology strategy significantly impacts a business's internal business processes and competitive advantage. These directly influence company efficiency and profitability, and technology directly relates to profitability. Astuti *et al.* (2018:327-329) also established that management support and information technology strategy, directly or indirectly, have a significant effect on internal business processes, competitive advantage, and financial and non-financial performance. Olutoyin and Flowerday (2016:7) concluded that an SME would be better positioned for successful technology governance if they carefully analysed the components of three key pillars: technological, environmental, and organisational.

Fortunately, Hoppe *et al.* (2021:254) found that improving the organisation's security culture can positively affect operational and technical vulnerabilities. Nevertheless, responsibilities and accountability should be clearly defined to inspire a security culture. It requires a people-centric strategic approach. Therefore security communication and

awareness campaigns should be a part of the organisation's security strategy (Hoppe *et al.*, 2021:254; Scholtz, 2019:4). The National Institute of Standards and Technology (NIST) in the US described awareness campaigns as far back as 2003 already (Wilson & Hash, 2003:8):

"Awareness is not training. The purpose of awareness presentations is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognise IT security concerns and respond accordingly."

Therefore, a business can gain a competitive advantage by combining people, quality information, and systems. Interestingly the vital link between these facets is the people.

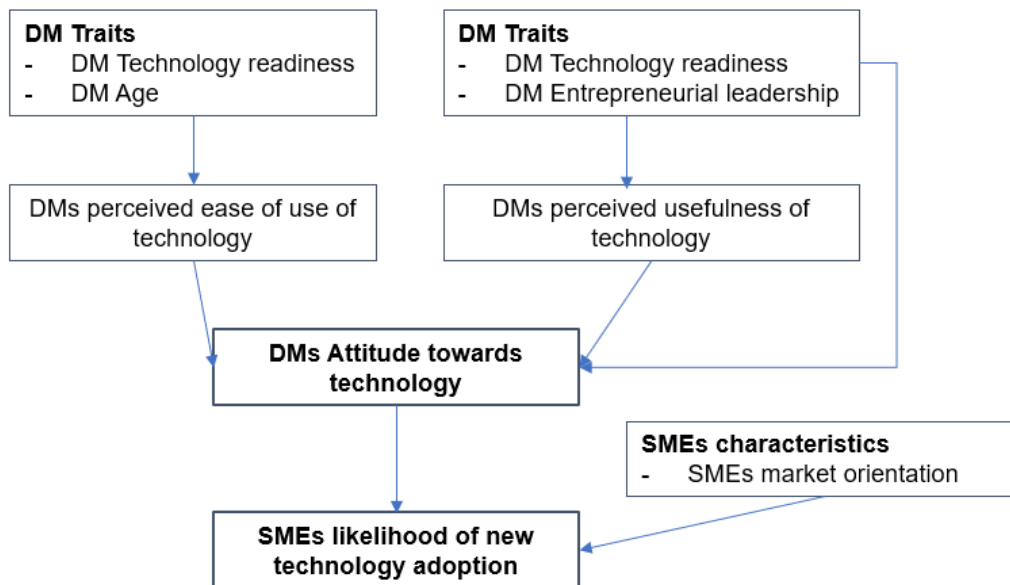
2.9 People, culture, and leaders

Digital transformation is not about replacing business processes but integrating people and technology into business and technology strategies (Artemenko, 2020:7-8). The organisation's internal data is the primary resource for enhancing and changing processes. The organisation's people remain the key to digital transformation, strategy integration, and vision and process implementation (Artemenko, 2020:4). As such, digital transformation is about both technology and employees. Georgiadou *et al.* (2020:9) highlight that the human factor is the most troubling threat in the business cybersecurity chain and, therefore, one of the most important. Decision-makers form the foundation of this weakness and cause critical cracks if they do not participate in discussions and be enlightened about their role. Georgiadou *et al.* (2020:9) concluded that when decision-makers are involved in discussions, they better understand the overall organisational security posture and implement the appropriate tools or models to mitigate risks. Armed with the knowledge and tools, they can securely navigate their business technology evolution.

Remarkably, internal traits such as technology readiness and the entrepreneurial spirit of decision-makers, as well as the company market orientation, are primary reasons for technology adoption possibilities within an organisation (Reynolds *et al.*, 2020:10). Reynolds *et al.* (2020:11) also found a positive correlation between the positive perception of technology of the leader and the likelihood of an organisation's adoption of technology. Moyo and Looock (2019:554) determined that the security perceptions of owners influence their decisions on technology system adoption. Interestingly, Reynolds *et al.* (2020:9) also established that the younger, more tech-savvy and entrepreneurial

decision-makers are, the more positive they perceive technology. They understand technical concepts more easily. Hence, they are more open to technology adoption and related discussions. Reynolds *et al.* (2020:12) further established that a decision maker's traits significantly impact the organisation's technology adoption tendencies, as depicted in Figure 1.

Figure 1: Impact of decision-maker (DM) traits on company technology adoption



Source: Adapted from Reynolds *et al.* (2020:12)

However, employees have to provide decision-makers with quality information within context.

2.10 Quality of information and processes

Naicker and Jairam-Owthar (2017:9) found that the quality of information has a solid mathematical influence on a leader's decision-making framework. (Naicker & Jairam-Owthar, 2017:3,9) further highlight the impacts of poor information quality, causing incorrect strategic decisions, wasted time, potential reputational harm, slow decision-making, and poor customer service. These inhibit the organisation's ability to operate. Jere and Ngidi (2020:7-8) further established that it is vital for leaders to be involved in first-hand technology discussions to grasp the context and extent of technology within their organisations. The context is a significant determinant in influencing the intention of

technology adoption, and leaders need to get first-hand, quality information to guide decision-making. Obtaining information from personnel delegated to technology discussions or cyber security is not enough. Intriguingly, Hodson (2019:xiv) suggests that top-level management misunderstands cybersecurity or IT principles because the IT and security teams are not contextualising information properly for management. Regardless, the risk responsibility still resides with the decision-makers. They must understand the risks and set strategies accordingly.

2.11 Competitive advantage

Business value innovation can either be hampered or improved through proper knowledge management in an organisation (Okanga, 2017:10). Aspects such as trend estimations can be hampered depending on leadership involvement or knowledge management (Naicker & Jairam-Owthar, 2017:9; Okanga, 2017:10). A Gartner hype cycle report expects that in the next two years, security rating service agencies will be able to provide a report on a company's security position to third parties for a relatively low cost. Albeit not a complete security audit, it will provide some insights into the organisation's security health and position. Insurance companies, competitors, customers or suppliers can use this data for vetting purposes before doing business. Similarly, Cybersecurity Maturity Assessments and Ethics and Compliance assessments can be used to assess an organisation before doing business (Zhang & Gopal, 2022). Therefore, organisations should start looking at IT security to create a competitive advantage instead of just seeing it as a cost centre and security risk.

In summary, Astuti *et al.* (2018:329) emphasise the importance of leadership involvement as follows:

"Suggestions for managers or executives of the company is to actively develop information technology in support of their work tasks according to their respective levels, to provide support for the use of information technology and its development and to understand information technology not only to facilitate the operational work of the organisation but also to support managerial decision-making and for competitive advantage."

Fortunately, if SMEs look at technology as an advantage and a tool, they can utilise it as a competitive advantage instead of looking at it purely as a risk or cost component. The involvement of leaders is vital in organisational information security and adoption

strategy. Security specialists conclude that the support of business leaders is essential to prepare for, and prevent, security breaches (Saban *et al.*, 2021:278).

In their “Global State of Information Security Report”, PricewaterhouseCoopers (2018) mentioned that senior leaders should take ownership of cybersecurity and manage information security in a top-down manner. According to Saban *et al.* (2021:278), information security should be a strategic priority in organisations that influence policies, procedures and, most importantly, the organisation's culture. All employees must understand the critical role information security plays in the organisation's success and sustainability. Also, factors influencing management's perception of information security should be a strategic priority in organisations.

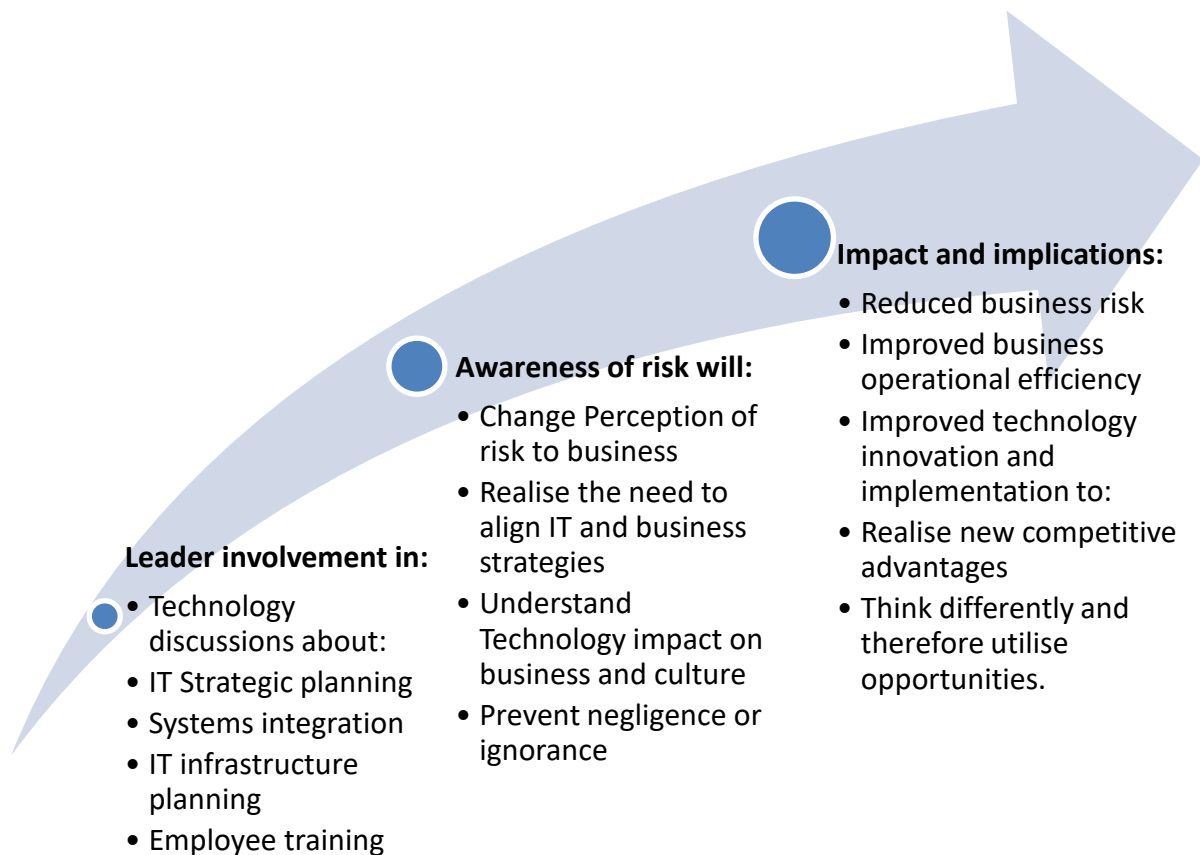
To handle the changing technology and business environments, organisations should incorporate technology into business risk management and understand its role in overall business and risk management (Marx & Schutte, 2018:61). Business leaders can no longer ponder whether they should digitalise or not. Schreckling and Steiger (2017:23) highlight that it is imperative and can be detrimental to a business. However, frameworks and models are available to guide SMEs with their digitalisation journey (Georgiadou *et al.*, 2020:9; Jere & Ngidi, 2020:7; Nel & Drevin, 2019:161; Schreckling & Steiger, 2017:19). Business leaders must be involved in all technical discussions to understand these digitalisation potentials and associated risks better.

Technology has changed the business world, defines business processes, efficiencies and overall competitive advantage, and is at the core of any business today (Schreckling & Steiger, 2017:23). Yet, the disconnect between a leader's technology readiness traits and perception of technology cause unnecessary risks to the business (Reynolds *et al.*, 2020:11-12).

2.12 Conceptual framework

The conceptual framework of this study, depicted in Figure 2, suggests that increased involvement or participation of decision-makers will affect their overall awareness of risk and opportunities within the business. The change in awareness will impact their risk perception of the business and can drastically change their approach to risk management and technology adoption.

Figure 2: Conceptual framework



2.13 The gap in evidence (The missing piece in related cases)

Technology is a vital component of business success. It can have a detrimental effect if not implemented properly. Instilling a security culture requires guidance from top-level management. Risk, risk management, culture, sustainability and competitive advantage are all business functions that leaders are responsible for in a business. The literature discussed highlights various risks, mitigation options and opportunities. However, none discuss the lack of involvement that leads to a lack of awareness of primary decision-makers in technology discussions. A leader can not make decisions based on these critical business aspects with second-hand information or delegate the responsibility. Doing so will open the SME up for potential losses, harm its reputation, reduce sustainability and limit opportunities.

2.14 Chapter summary

This chapter discussed the impact, and potential benefits cybercrime has on SMEs. An interesting narrative arises from the literature, namely the importance of culture in the

cybersecurity environment of SMEs. The leaders of an organisation are responsible for establishing and maintaining the organisation's culture. They are also responsible for risk management, competitive advantage, sustainability, and supply chain management of the organisation. As discussed, all aspects are affected by cybercrime and risks. However, if the primary-decision makers are not aware of these risks or do not incorporate these risks into the strategic processes of the organisation, it creates a big vulnerability for SMEs. Lastly, the chapter closes with the conceptual framework and the gap identification to indicate the effect of involvement on awareness, which in turn affects risk perception and, ultimately, the impact on business success.

The following chapter describes the philosophy and strategies utilised in this study and explains the scope of the study in detail.

CHAPTER 3: RESEARCH DESIGN AND METHODS

3.1 Chapter introduction

Chapter 3 defines the quantitative research methods used to conduct this study, detailing the population and sample process, the research instruments used, and the statistical methods applied to analyse the data. Reliability, validity and ethical concerns are also clearly specified.

3.2 Research philosophy and paradigm

According to Saunders, Lewis and Thornhill (2019:166), quantitative research characteristics are typically positivist philosophy if used with highly structured, predetermined data collection techniques. It is usually associated with a deductive approach to use data to test the theory and examine the relationship between variables. It is measured numerically and analysed using various statistical and graphical techniques. Additionally, as with experimental designs, they use controls to ensure data validity and use a single data collection technique, such as a questionnaire. Saunders *et al.* (2019:181) further explain that a quantitative experiment with only one group where all participants are exposed to the same intervention is known as a within-subject design and uses a repeated-measures approach.

This study will test theories about the relationship between leadership's involvement in technical discussions and the impact on perceived business risk. Thus, it will use the quantitative philosophy with a deductive approach to test proposed hypotheses (Bryman *et al.*, 2014:32). The participants will be presented with a questionnaire to get a baseline of the variables and provide an information session to all participants. After the session, all participants will complete core questions again to test a change in the variables. Therefore, this study will utilise a quantitative, experimental within-subject design and implement a repeated measure approach on all study subjects. The relationship between involvement and perceived risk to business will then be tested between the questionnaires.

Therefore, this study will be an experimental quantitative study to test hypotheses by collecting primary, structured data to determine the dependent and independent variables' significance. This study complies with the characteristics of a quantitative study with a deductive approach and positivist philosophy (Bryman *et al.*, 2014:31).

3.3 Research strategy

An experiment studies the probability of a change in an independent variable causing a change in another dependent variable (Saunders *et al.*, 2019:178). This experimental study utilizes questionnaires and presents information to manipulate the independent variable (leader involvement), testing the influence on the leaders' perceived risks to the business (the dependent variable).

3.4 Research choices

The study utilised one type of structured questionnaire, and then data will be analysed with SPSS (Version 25.0) software. Therefore it will be a mono-method quantitative study (Saunders *et al.*, 2019:166).

3.5 Technique and procedure

According to Bryman *et al.* (2014:101), an experimental study determines the correlation between an independent and dependent variable. A quasi-experiment is where respondents will be presented with the same information to determine the change in approach towards technology decision-making. As hypothesised, the decision-maker's involvement is the cause or the independent variable that will influence the risk to their business, which is the dependent variable or the effect.

Bryman *et al.* (2014:101) emphasise that the researcher should manipulate the independent variable to conduct an experimental study. The respondents are the independent variables and are manipulated by providing an information session to change their perception and level of knowledge about technology risks to their businesses. In turn, the perception of risk in the business is the dependent variable, possibly due to the leader's lack of involvement or knowledge about technology risks.

3.6 Study population and sampling

3.6.1 Defining the population

The population will consist of the primary decision-makers in small and medium-sized businesses confronted with security and technology adoption decisions in their business. These businesses have full-time employees who use computers daily.

3.6.2 Sample

When it is unrealistic to collect data from the entire population, a sample can be selected to represent the entire population to generalise the results (Saunders *et al.*, 2019:274). As it is not realistic to obtain data from every SME decision-maker in the North West and Gauteng areas, a sample will be selected to present the population.

For this study, the sample will consist of the following:

- Primary technology decision-makers,
- of SMEs registered with a chamber of commerce,
- or registered as part of alternative initiatives of these chambers of commerce,
- in the North West and Gauteng provinces of South Africa,
- with employees who work on computers daily

Probability sampling can be used when everyone in the population has an equal opportunity to partake in the study, and is often associated with experimental studies (Bryman *et al.*, 2014:173); Saunders *et al.* (2019:275-276). This study used probability sampling because all members of the selected chambers of commerce in the North West and Gauteng province had an equal chance to participate, regardless of industry or background. A probability sample represents the population, eliminates bias, keeps sampling errors in check, and allows statistical significance (Bryman *et al.*, 2014:171).

The researcher advertised the need for respondents as part of the free information session through the chamber of commerce to obtain respondents from the sample. The free information session will provide detailed steps to improve the overall risk profile, mitigation steps, and clear preventative measures for the inevitable cyber-attack or virus.

3.6.3 Sample size

Maree (2016:199) notes that a smaller sample size may represent the population adequately in populations where population members are similar concerning the study's variables. Additionally, a smaller sample will be sufficient in simpler models that represent the population and where the variety of respondents is low (Bryman *et al.*, 2014:176-177; Maree, 2016:199). According to Saunders *et al.* (2019:280), a sample size of at least 30 is sufficient in smaller studies.

Due to the inadequate response from the Potchefstroom Chamber of Commerce members, the researcher expanded the sample to include decision-makers from businesses registered with the GTCoc (The Golden Triangle Chamber of Commerce) and Matlosana chambers of commerce. The sample size for the Potchefstroom chamber was (n=120), for the ProPotch initiative (n=60), and for GTCoc (n=156), totalling 336 possible respondents as part of the study population.

The study focused on decision-makers of SMEs, and hence respondents are very similar with low variety. Consequently, a smaller sample will be sufficient, as indicated.

3.6.4 Inclusion criteria

- Primary decision-makers of technology adoption and risk management in SMEs.
- They can be the owner or manager but must be a person involved in making the final decision regarding technology adoption and strategy within the organisation.

3.6.5 Exclusion criteria

- Employees responsible for technology management or planning but not the final decision-maker relating to the adoption or implementation of technology will be excluded.
- Enterprise companies because they tend to have dedicated C-level information technology specialists employed who are involved as part of their job description.

3.6.6 Sample limitations or errors

- Primary decision-makers are busy and have limited time to answer research questionnaires. Therefore, the response was much lower than expected.
- Even increasing the sample to include two additional chambers, the Golden Triangle Chamber of Commerce and the Matlosane chamber of commerce, did not help to increase the participation by much.

3.7 Relationship between the researcher and the participants

The researcher kept the interaction between respondents and himself to a minimum to ensure unbiased results. The information session was a pre-recorded session that

respondents could watch at leisure. The session provided standardised information to participants and, therefore, was easily repeatable and thus reliable.

3.8 Recruitment of potential respondents

Respondents received an email from the chamber of commerce communication channels with a link to the survey questionnaire, including a link to the information session. The information sessions provided material on the risks to businesses, mitigating these risks and providing strategies to minimise losses when such security events occur. A consent form was attached to ask for their participation with more detail, including the purpose of the study, ethical matters, and instructions to complete the questionnaire.

3.9 Measuring instruments and data collection

The measuring instrument was an online, self-completed, closed-ended and structured questionnaire to collect the primary data needed to achieve the study's objectives. To measure the dependent variable's change, the respondents completed the questionnaire before the information session to obtain a baseline and then again after the information session. This type of test is known as a repeated measures approach (Saunders *et al.*, 2019:181). The researcher created the questionnaire from existing validated instruments and consulted current literature to further adjust for this study.

The questionnaire contained two primary sections. Section A presents multiple-choice questions to acquire demographic information about the respondents and their businesses. Section B uses a 7-point semantic differential scale with 25 questions where respondents can indicate their level of agreement with statements to measure the variables.

With the questionnaire, the researcher obtained the primary data from respondents in a phased approach set out below:

1. Invited business owners and leaders to complete the questionnaire and view the information video in the form of a pre-recorded session.
2. The webinar or recording provided:
 - a. Insights into the risk landscape to businesses, highlighting various types of internal and external threats.

- b. Compliance requirements and related reputational or financial damage if not compliant. Also, point to the benefits if you do comply and how to utilise them.
 - c. Show the impact on business competitiveness and success if leaders do not consider these risks in the business strategy. These were both positive and negative.
 - d. Action steps to mitigate these risks and minimise the impact of attacks or problems.
 - e. Finally, it provided strategies to minimise losses when disaster events do occur.
3. Once the respondents finish the recording, they will complete the core questions of the questionnaire again.
 4. The participant's email address was used as a unique identifier to track the response between the first and second questionnaire

3.10 Reliability and validity

Reliability relates to the consistency of results from the same questionnaire conducted at different times under the same conditions. Individuals or sets of items should produce consistent results in line with the overall questionnaire (Field, 2009:673-674). Therefore reliability determines how much the results can be generalised to a larger context.

Validity refers to whether the measuring instrument measures what it is supposed or designed to measure (Bryman *et al.*, 2014:38; Field, 2009:674; Maree, 2016:239). Reliability is confirmed because the questionnaire is a repeated measures type test (completed twice), and the two tests were done more than a week apart to address the negative “memory effect” of this test (Maree, 2016:238). Some questions were stated negatively and were sourced from previous studies at face validity to address validity concerns (Maree, 2016:240-241).

3.11 Data and statistical analysis

According to Bryman *et al.* (2014:320); Field (2009:175), a bivariate analysis is used to analyse the relationship between two variables.

This study analysed the linear correlation between the respondent's involvement in technical discussions and the resulting perceived risk to the business. Therefore, a bivariate analysis is appropriate. The researcher approached the North-West University Statistical Consultation Service to correctly capture and analyse the data. Descriptive and relational statistics were performed with IBM SPSS (Version 25.0) to test the hypotheses with:

- Data reduction through exploratory factor analyses would have been performed to ensure the reliability of the variables. Cronbach's alpha coefficients calculate the average of all possible split-half coefficients. The calculation of this coefficient varies between 0 and 1, thus between no correlation (not internal consistency) and perfect correlation (complete internal consistency) (Bryman *et al.*, 2014:38). Unfortunately, due to the low number of respondents (n=36) factor analysis and reliability tests was not viable.
- Means, standard deviations, and an overview of variables were done instead.
- Spearman's rho correlations will confirm the variables' relationships, and t-Tests were used to test the differences between samples (p_1 and p_2).
- The Wilcoxon and Mann-Whitney tests are the non-parametric versions of the dependent and independent T-tests, which are more appropriate for small studies. These will reflect the effect size of the difference between groups or variables.

3.12 Ethical issues and informed consent

The first page of the online questionnaire explains the study's background and reason and comprises an informed consent form. Respondents have a choice to accept the conditions of the study and consent to the usage of their data. In line with ethical requirements and the Protection of Personal Information Act (PoPIA) code of conduct, as described by Adams, Adeleke, Anderson, Bawa *et al.* (2021:1-10), the consent on the first page of the online questionnaire as attachment Addendum A include:

- The reason for the study.
- What personal and social information will be collected, and why is it required for this study?

- Who will access the data, how will it be stored (for how long) and safeguarded, and how will it be used?
- Explain the ethical clearance for the study with the relevant references and contact details.
- Explain how the researcher maintains confidentiality and anonymity and how data, information, research results, and data storage will be maintained.
- Highlight that research results will not include any identifiable data when published.
- Explanation of the detailed process to participate in the study and what respondents can expect.
- Estimated time it will take to complete the questionnaire and information session.
- Confirm voluntary participation in the questionnaires and information session.
- Highlight that respondents can opt out of the study process at any time.
- Contact information will be available for respondents to lodge complaints if they feel the questions are too intrusive or unethical.
- Explain that data will be analysed with appropriate statistical software and experts at the North-West University Statistical Consultation Service.

3.13 Other ethical considerations

- Due to the online nature of the study, no access is required to premises or respondents directly, and invasion of privacy is not a concern.
- Participants were not disadvantaged, regardless of whether they completed the process. If they do not complete the questionnaires, they will still have access to the information session recording.
- If an existing respondent provides a reference, the respondent must obtain consent before sharing the reference details. The reference will follow the same process of providing consent before participating in the study.
- It was explained that data from the respondents will only be used for this study and will not be used for any other study in future without additional consent as required per PoPI Act (Adams *et al.*, 2021).

3.14 Chapter summary

This chapter started by describing quantitative research characteristics and which applied and were utilised in this study. It further explained the requirements needed to measure and test the relationship between the involvement of leaders and their risk perception. Additionally, it explained how the data was analysed to ensure reliability, validity and ethical standards and, consequently, valuable research results. The next chapter will discuss the results and present the findings.

CHAPTER 4: DATA ANALYSIS AND DISCUSSION OF FINDINGS

4.1 Chapter introduction

This chapter discusses analysing the data from the seven-point Likert scale questionnaires. The questions were split between the involvement section measuring never (1) and always (7) and the risk section rating between low (1) and high (7). The first part of the results will discuss the demographics and background questions of the respondents, and the second will elaborate on descriptive and frequency statistics.

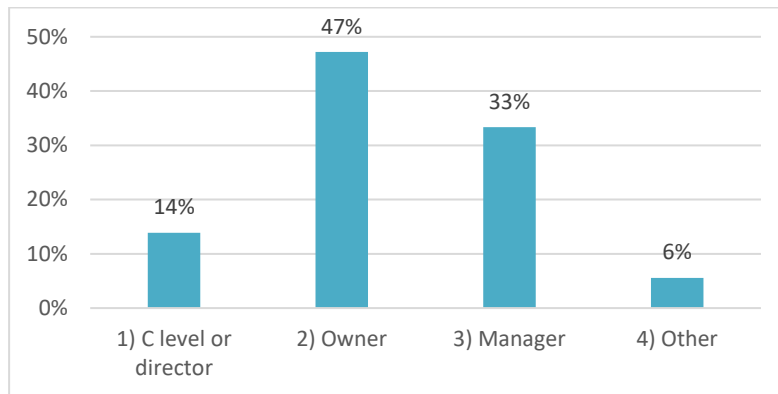
The third section will discuss the Dependent and Wilcoxon signed rank test to compare the pre and post-test results and highlight the significance between the results with appropriate effect size. The Independent and Mann-Whitney tests will compare results from demographic groups. The final 4th section will explain the correlations between the questions using Spearman's rho. The effect size results in this section will address some limitations of a small quantitative study, as it shows significance regardless of the size of the study (Maree, 2016:233). From the initial sample (n= 336), the response rate was low, with 36 responses on the first questionnaire and 16 on the follow-up questionnaire.

4.2 Demographics and background

Only 15 of the respondents indicated that they are 40 years or younger. Twelve respondents, almost a third of the sample, indicated that they are 41-50 years old. The remaining nine respondents were 51 years and older.

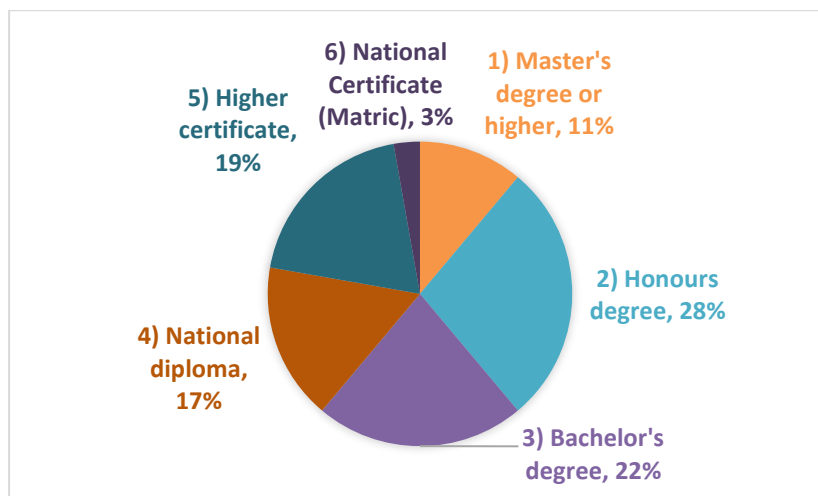
Concerning the respondents' position or affiliation at the business, depicted in Figure 3: 5 respondents indicated C level or director (14%), 17 respondents indicated that they are the owner of the business (47 %), 12 respondents indicated that they are the manager of the business (33%) and two respondents selected the other option (6%). Therefore 61% of respondents (Owner, C-level or director) represent the primary decision-makers in their respective businesses.

Figure 3: Position at company



Regarding education level, Figure 4 shows that 22 (61%) of respondents had a degree or higher, with 8 (22%) having a bachelor's degree, 10 (27%) noting an honours degree and 4 (11%) having a master's degree. Another 13 (36%) indicated a national diploma or higher certificate level, with only one respondent having a national certificate (Matric).

Figure 4: Level of education

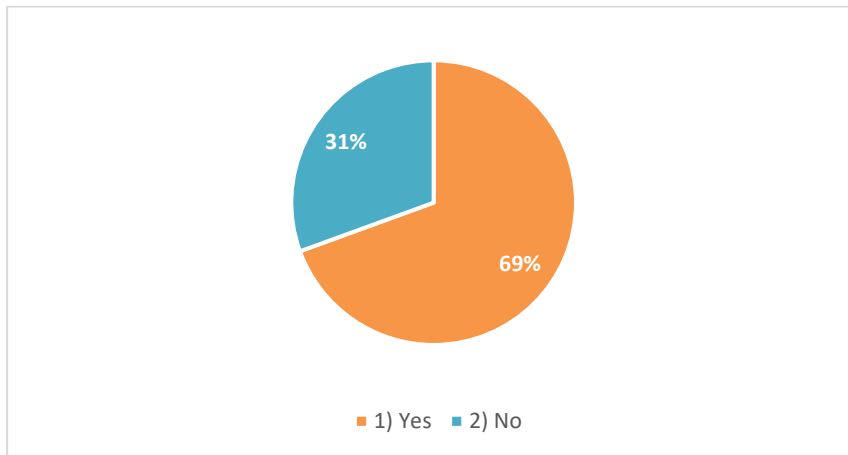


As regards business size, the most prominent representative group participating was the 20-40 employee group, with 12 (33%) responses. The second largest was the 1-5, indicating self-employed or micro businesses with 9 (25%). The 11-20 group had only 7 (19%), 2 in the 50-100 range with only 1 in the medium business size of 250+.

Of the respondents, 16 (44%) said the businesses they represent had been in operation for more than 20 years, 8 (22%) for 11-20 years, 6 (17%) for 6-10 years and another 6 (17%) for less than five years.

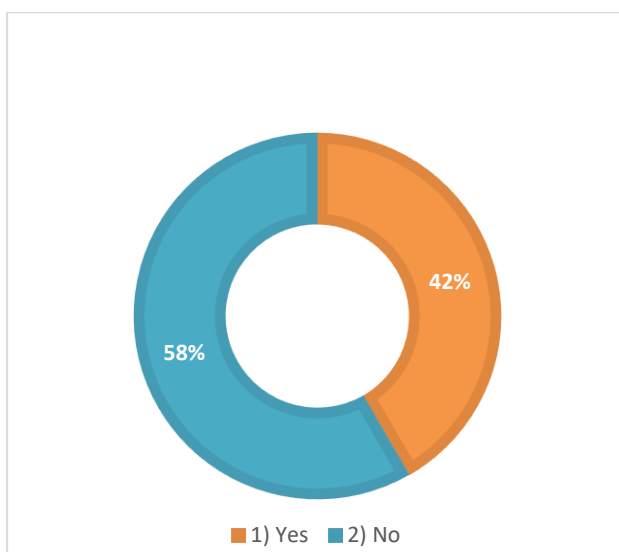
Of the 36 respondents, 25 (69%) indicated that they are the primary decision-makers in the respective organisations they represent, as depicted in Figure 5.

Figure 5: Primary decision-maker



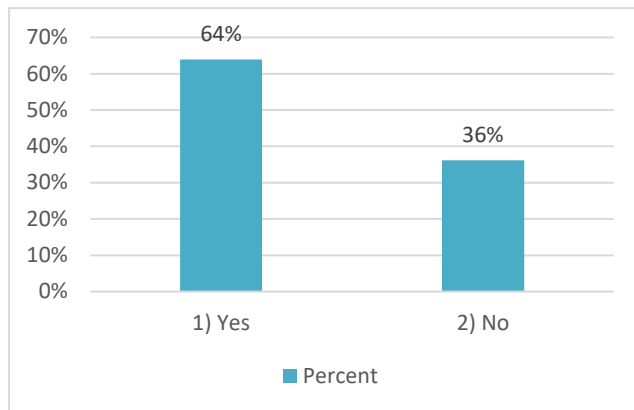
Interestingly, when asked if the organisation the respondents work for (represent) had previously experienced cyber attacks or ransomware, 15 (42%) indicated yes, and 21 (58%) specified no, as presented in Figure 6, thus highlighting a high risk of cyber attacks in local SMEs.

Figure 6: Previous cyber attacks experienced



Fortunately, 23 (64%) indicated that their respective organisations have a security policy, as shown in Figure 7, which is a good starting point for cybercrime awareness.

Figure 7: Security policy in place



30 of the 36 respondents represented businesses registered with a chamber of commerce, and six did not mention which initiative or chamber. Of the 30 respondents, 22 (64%) represented businesses registered with the Potch-Tlokwe Chamber of Commerce, 6 (16%) with the Golden Triangle Chamber of Commerce and only one with the Matlosane Chamber of Commerce.

4.3 Frequencies and descriptive statistics

4.3.1 Involvement

This section discusses the frequency and descriptive statistics results regarding the involvement section of the questionnaire.

Table 1: Involvement Frequency statistics summary

Question number	N	Minimum	Maximum	Mean	Std. Deviation
Q15	36	1	7	6.08	1.44
Q18	36	1	7	3.03	1.93
Q17	36	1	7	5.36	1.79
Q19	36	1	7	3.58	1.87
Q21	36	1	7	5.44	1.90

Regarding the statements for the involvement section summarised in Table 1, the lowest means were for Q18, stating that *"I regularly attend webinars or seminars about technology risks to businesses"* (mean = 3.03; SD = 1.93) and 58% below 3 (out of 7), indicating that respondents, on average, are uninterested and leaning towards never. Additionally, the statement of Q19, *"I regularly read about technology and cyber security risks to the business"* (mean 3.58; SD = 1.87), similarly indicates low interest, with 53% of respondents indicating a value of less than 3 (out of 7). The highest mean was reported for Q15, stating, *"I consider IT tools and security an essential organisational priority"* (mean = 6.07; SD = 1.44) and only 8% below 3 (out of 7), indicating that respondents, on average lean towards always. Similarly, the means for Q17, *"Our business takes IT tools and security into account when planning business strategies,"* and Q21, *"I am aware of the positive impact of IT tools and security on business competitiveness,"* were relatively high at 5.44 and 5.46, respectively. The results reflect that respondents know and consider IT tools and security essential priorities for success. However, they contradict this by not deeming it vital enough to attend information sessions or reading up on security risks to educate themselves and be more aware of the risk and impact on the business.

Q13, *"Primary technology decision-makers are always involved in technical discussions with the IT team or contractor about related technology and security for the business"*, has a high mean (mean = 5.69; SD = 1.79), which shows that most respondents consider primary decision-makers representing their respective businesses to be present in IT discussions.

Q16, *"I prefer to delegate technology discussions to other employees as the technical language frustrates me"*, had a mean of 3.69 (SD = 2.0), indicating that respondents are

split in two and do not lean primarily to any one side. Nevertheless, 39% of respondents leaned towards “always” delegating technology discussions, showing that several leaders can be uninformed due to not attending the discussions.

Although Q20, *“I am aware of technical challenges experienced by employees and how to improve them”*, has a relatively high mean (4.75; SD = 1.80), the fact that 19% lean towards never (3 and below) shows an unawareness of the frustration experienced by employees regarding information systems and technical environment, thus reducing productivity and efficiency in the organisation.

4.3.2 Risk

This section will discuss the descriptive and frequency results regarding the risk section of the questionnaire.

Q22, *“Technology security and cyber-attacks pose a significant risk to the business”*, has a high mean (5.28; SD = 2.19), highlighting that most participants consider cyber-attacks a significant business risk. Still, 25% leaned towards “low”, highlighting the gap in perception regarding business risks.

Q23, *“IT tools and security is a waste of money as protection cannot be 100% secure”*, with a mean of 2.11, and **Q25**, *“Technology and related security is merely an expense item,”* with a mean of 2.50, were negatively stated to test the negative perception towards IT and related security requirements. With these low means, respondents rejected the idea that IT and related security is merely a waste of time and not seen as a wasteful expense, although six respondents indicated the reverse.

Q33, *“The business has an IT security policy and recovery plan in place and is updated regularly?”* with a mean of 4.31 (SD = 1.91) is concerning, especially since 30% indicated below 3, leaning towards “low”. At least a few respondents’ businesses know about and implement these vital processes.

Of concern is that **Q34**, *“Aware of insurance products against potential losses of data or cyber-attacks”*, ranked low at a mean of 3.86 (Pre-test), with 39% leaning towards “low” awareness. However, there is a practically visible correlation (0.36) between the awareness of insurance products and the organisation's size, with a significant statistical relationship (0.031). Thus, decision-makers are mainly unaware of insurance options for when a cyber-attack occurs, which can cause significant damage to the business without

insurance options to mitigate the impact. Again, these indicate that a lack of awareness can result in unnecessary losses and minimal mitigation options.

A significant concern is how low respondents ranked **Q29**, "Indicate the likelihood that the business will experience a cyber disaster event in the next year", with a mean of 2.94 in the pre-test (N=36). Q29 was also the lowest mean in the risk section of the questionnaire. However, 42% of the respondents indicated in Q9 that their respective businesses had previously experienced cyber-attacks. Additionally, **Q30**, "Indicate the level of risk to the business sustainability and competitive advantage if a cyber disaster event does occur," had a mean of 4.92, indicating that respondents perceive the risk to business sustainability as relatively high if such a disaster event should occur. However, 27% of respondents indicated a risk level below 3 (of 7), representing that it will not drastically impact their business.

Interestingly, most respondents understand the implication of technology security related to PoPI Act compliance in Q36, "*I / the business is fully aware of PoPI Act and related technology requirements and fines*", with a mean of 5.81, and Q37, "*Technology security is a foundational aspect for businesses to be PoPI Act compliant*", with a mean of 5.94. The mean for Q37 was also the highest in the Risk section in both pre-and post-tests. Hence, it indicates that decision-makers are more aware of the risks and perceive them differently because they have increased responsibilities due to enforcing regulations and fines.

4.4 T-tests, Wilcoxon and Mann-Whitney tests

4.4.1 Dependent t-test and Wilcoxon test

The Dependent and Wilcoxon signed rank test would compare the pre and post-test results and highlight the significance between the results with appropriate effect size.

The dependent samples t-test compares the sample means from two related groups in a pre-and post-test experimental scenario (Maree, 2016:250-252). It compares the results of two questionnaires from the same respondents. This test aims to determine if there is a change from one measurement (group) to the other, thus highlighting the potential difference the information session might have had on respondents.

The Wilcoxon signed rank test is the non-parametric version of the dependent samples t-test and uses ranked or ordinal data. This test is appropriate if the sample size is small (<30), as in this study (Maree, 2016:256). The interpretations will be based on the effect sizes with the following guideline values for interpretation.

- **Guideline values for the t-tests:** 0.2 practically non-significant difference, 0.5 practically visible difference, 0.8 practically significant difference (Maree, 2016:233-234).
- **Guideline values for the Wilcoxon signed rank and Mann-Whitney test:** 0.1 practically non-significant difference, 0.3 practically visible difference, 0.5 large, practically significant difference (Maree, 2016:234, 256).

The effect size and the p-values highlight the scale of the difference or correlation being tested, which is not affected by the study size (Maree, 2016:233). Therefore, the effect size will still be appropriate in discussing differences and correlations in this small study.

In the dependent and dependent t-tests, Wilcoxon signed rank test, and Mann-Whitney tests, p-values are generally reported for completeness, but this study will not interpret these since a convenience sample was used instead of a random sample.

4.4.2 Result: IT tools and security as a waste of money

Q23 is stated **negatively**: *"IT tools and security is a waste of money as protection cannot be 100% secure."*

Table 2 shows the results of the Q23 Dependent t-test and Wilcoxon signed rank test.

Table 2: It tools and security as a waste of money

Question	Measurement	Descriptives			Dependent t-tests		Wilcoxon Signed Ranks Test	
		N	Mean	Std. Deviation	p-value	Effect size	p-value	Effect size
Q23	Pre	16	2.44	1.71	0.167	0.33	0.20	0.32
	Post	16	1.88	0.89				

Although the effect size of the t-test leaning towards practically visible difference (0.33), the Wilcoxon ranks test effect size indicates a practically visible difference (0.32) between the means of the pre and post-tests for Q23. The pre-test has a mean of 2.4 (SD 1.71), whereas the second declined (improved) to 1.88 (SD = 0.89), noting that the values ranged from 1 (Never) – 7 (Always) and this question was stated in a negative manner. Therefore, the results indicate an increased awareness of how vital IT tools and security is for a business.

4.4.3 Result: Cyber disaster likelihood

Q29 *"Indicate the likelihood that the business will experience a cyber disaster event in the next year."*

Table 3 shows the results of the Q29 Dependent t-test and Wilcoxon signed rank test.

Table 3: Cyber disaster likelihood

		Descriptives			Dependent t-tests		Wilcoxon Signed Ranks Test	
Question	Measurement	N	Mean	Std. Deviation	p-value	Effect size	p-value	Effect size
Q29	Pre	16	3.25	1.61	0.167	0.35	0.19	0.32
	Post	16	3.81	1.80				

The effect size of the t-test indicates a that the difference is leaning towards being practically visible. (0.35), but the Wilcoxon ranks test indicates a practically visible difference (0.32) between the pre and post-test for Q29. The pre-test has a mean of 3.25 (SD 1.61), whereas the post-test increased (improved) to 3.81 (SD = 1.80). It is a significant concern that the majority think that the likelihood of experiencing a cyber disaster is so low, although 42% of respondents indicated that their businesses had experienced a cyber-attack before, thus revealing a gap between the perception of risk and the likelihood.

4.4.4 Result: Cybersecurity training

Q32 *"Is cybersecurity training a priority in the business?"*

Table 4 shows the results of the Q29 Dependent t-test and Wilcoxon signed rank test

Table 4: Cybersecurity training

		Descriptives			Dependent t-tests		Wilcoxon Signed Ranks Test	
Question	Measurement	N	Mean	Std. Deviation	p-value	Effect size	p-value	Effect size
Q32	Pre	16	3.31	1.40	0.145	0.54	0.12	0.39
	Post	16	4.06	1.95				

Based on the effect sizes of the t-test (0.54) and the Wilcoxon test (0.39) for Q32, there is a visible practical difference between respondents' opinions before and after the information session. Before the information session, respondents indicated a mean of 3.31 (SD = 1.40). After the session, they indicated 4.06 (SD = 1.95). The results indicate that the priority regarding cybersecurity training increased after the information session.

4.5 Independent t-test and Mann-Whitney U Test

The Independent and Mann-Whitney tests will compare results from demographic groupings.

The independent t-test determines whether there is a difference between the means in two unrelated groups. The validity of the t-test depends on the difference in the variance of the variable in the two groups (Maree, 2016:251). This test was used to test differences between demographic groups.

The Mann-Whitney U Test is a non-parametric equivalent of the independent statistical samples t-test used to compare two samples or independent groups based on a single variable (Maree, 2016:258).

4.5.1 Result: Previous cyber-attack against the likelihood of happening

Table 8 displays the results of Q29 grouped depending on whether the respondents indicated that their organisations previously experienced an attack (Yes or No). Groups are tested against the likelihood of it happening in their current business or again in the next year.

Table 5: Test results for previous cyber-attack experiences and likelihood

		Descriptives			Independent t-tests		Mann-Whitney Test	
Question	Measurement	N	Mean	Std. Deviation	p-value	Effect size	p-value	Effect size
Q29	Yes	15	3.40	1.50	0.161	0.47	0.11	0.27
	No	21	2.62	1.66				

There is a practically visible difference between means of Q29, “Indicate the likelihood that the business will experience a cyber disaster event in the next year” between respondents saying yes and no on Q9, “Our business experienced one or more cyber-attacks or ransomware before”, with n t-test effect size of 0.47 ($p = 0.161$) and a Mann-Whitney effect size of 0.27 ($p = 0.11$). The mean for the Yes group is 3.40 (SD = 1.50) and 2.62 (SD = 1.66) for those that indicated No. Thus, respondents who previously experienced a cyber-attack find it much more likely that the business will experience another attack.

4.5.2 Result: Delegate tendency depending on the position

To gain more insights into respondent opinions based on their position at the organisation 2 groups were formed:

- The “C-level or director and Owner” group includes respondents from the “C-level or director” and “Owner”; and
- The “All other” group include respondents from the “Manager” and “other” grouping.

Table 6 depicts the independent T-test results of Q16 “*I prefer to delegate technology discussions to other employees as the technical language frustrates me*”, comparing the position groups at the company.

Table 6: Delegate tendency independent T-test, depending on the position

Question	Position_grouped2	N	Mean	Std. Deviation	Effect size
Q16	C-level or director and Owner	22	4.05	1.838	0.41
	All other	14	3.14	2.179	

The C-level, directors and owners group has a mean of 4.05 (SD = ...) and the manager and other groupings a mean of 3.14 (SD = ...) , with a practically visible difference (effect size = 0.41). Hence, C-level, directors and owners indicated that they more often prefer to delegate technology discussions to other employees as the technical language frustrates them

4.6 Correlations

The Spearman's rho correlations test indicates the practical significance of the relationship between variables or effect sizes where at least one variable is ordinal (Bryman *et al.*, 2014:321). It uses ranks instead of actual values and does not assume the distribution of the variables (Maree, 2016:267). The guideline values are ~0.1, small, no significant practical correlation; ~0.3, medium, practically visible correlation; ~0.5, large, and practically significant correlation.

4.6.1 Result: Awareness

The correlations between:

1. Q13 (Primary technology decision-makers are always involved in technical discussions with the IT team or contractor about related technology and security for the business)

and

1. Q19 (I regularly read about technology and cyber security risks to the business),
2. Q21 (I am aware of the positive impact of IT tools and security on business competitiveness.),
3. Q28 (I Understand the impact IT tools and security have on business success.), as well as

4. Q30 (Indicate the level of risk to the business sustainability and competitive advantage if a cyber disaster event does occur),
 5. Q35 (Technology adoption and innovation is a driver for business success in future),
- are all practically significant ($r = 0.502 - 0.619$). These positive correlations indicate that respondents indicate high for Q13. They also indicate High for the other questions. The correlation indicates increased awareness of cyber risk to the business, positive impact of IT tools in the business, risk perception to the business, and potential drivers for success, depending on the involvement of the primary decision-makers.

4.6.2 Result: Awareness

In terms of the impact of cybercrime, the risk to the business and the advantages of technology are practically visibly correlated with the size of the organisation, as indicated in the following:

Q17 - Cyber planning

Q21, 28 - The impact of IT tools on risk and success to the business

Q22 - Cybercrime risk to business

Q30 - Impact on sustainability and competitive advantage of cyber risks

Q31 - Preparedness of business in the event of cyber-attack

Q32 - Priority of cybersecurity

Q34 - Awareness of insurance products for cybercrime

Q35 - Technology as a future business success driver

Hence, indicating that the size of the business influences these aspects.

There is a practically visible correlation between the awareness of insurance products and the organisation's size (0.36) for **Q34**, "*Aware of insurance products against potential losses of data or cyber-attacks*", with a significant statistical relationship (0.031), thus indicating that larger organisations might be more aware of these options.

4.6.3 Result: Technical understanding

Questions Q14, Q15, Q18, Q19 and Q21 relate to the technical understanding and awareness of the respondent based on interest, reading and attending information sessions regarding cyber-risks. Respondents who indicated high for Q14, “I am interested in security issues and mitigation options”, also indicated high for:

Q22, “Technology security and cyber-attacks pose a significant risk to the business” (0.432),

Q24, “How concerned is the organisation about IT and cyber security?” (0.466),

Q26, “How much of a risk is cybercrime to the business ”(0.407), and

Q27, “How much of a risk is cybercrime to yourself” (0.480).

The results all lean towards a large, practical significant correlation with these questions, which are all related to risk perception, thus indicating that interest in security and mitigation options does correlate with risk perception.

4.6.4 Result: Technical understanding

Q19, “*I regularly read about technology and cyber security risks to the business*” speaks to the technical understanding of the respondent. Q19 has a large, practically significant correlation between (0.49 to 0.664) with:

Q15, “*I consider IT tools and security an essential organisational priority*”,

Q17, “*Our business take IT tools and security into account when planning business strategies*”,

Q18, “*I regularly attend webinars or seminars about technology's impact on businesses*”,

Q24, “*How concerned is the organisation about IT and cyber security?*”, and

Q28 “*I understand the impact IT tools and security have on business success.*”

These results indicate that a more technically inclined or informed person better understands how IT tools and security might impact business success and risks. They might be more cognisant of these factors and more willing to participate in the discussions. Interestingly, Q19 is one of only two questions that correlate significantly with Q18, indicating that those who regularly read about technology and cyber risks tend to be more engaged with other content about cyber security.

4.7 Discussion

Q23 (11.2.2; 11.3.1) and Q25 (11.2.2) results indicate that respondents mostly regard technology as an essential business component by rejecting the negative statements that it is a waste of money and merely an expense item. Furthermore, the results from Questions 14 (section 11.5.3) and 19 (11.2.1; 11.5.1; 11.5.3; 11.5.4) indicate that those respondents who are interested in, read up on and are more involved or aware of security and risk issues in their business might have a different risk perception due to increased awareness.

Nevertheless, it is a significant concern that most respondents in the pre-test think the likelihood of experiencing a cyber disaster is low in Q29 (11.2.2; 11.3.2; 11.3.4), especially while 42% of respondents indicated that their businesses had previously experienced cyber-attacks. However, the results indicate a visible increase in the perception of respondents' likelihood of a cyber disaster event for their business after the post-test. As the t-test results indicated regarding Q9 against Q29 (11.3.4), decision makers' perception changes towards the likelihood of an attack, and thus the risk to the business, only after a disaster event occurs. Consequently, the results reveal a gap between risk perception and the likelihood of experiencing an attack. This finding corresponds with the literature section indicating that required change only happens after experiencing losses due to a cyber disaster event or data corruption (Keeper, 2021:4).

Fortunately, SMEs can mitigate these losses through Cyber insurance products, though respondents indicated a low awareness of such products in Q34 (11.2.2; 11.5.2) results. However, insurance will not help prevent downtime, loss of data or reputation but merely mitigate the immediate financial loss incurred for recovery and investigation purposes (Hoppe *et al.*, 2021:254). Unfortunately, 38.9% of respondents are unaware of insurance options for when a cyber-attack occurs, which can cause significant damage to the business. Interestingly, there is a practically visible correlation between the awareness of insurance products and the organisation's size, with a significant statistical relationship representing that larger organisations might be more mindful of such products to mitigate the cyber-attacks impact.

The results for Q16 (11.2.1; 11.4.1) are troubling, though, considering that 39% of respondents leaned towards "always" delegating technology discussions to other employees, especially for the C level, directors and owners of organisations. These results might be logical, as leaders are typically very busy delegating tasks that might not

be of critical importance or interest to the person. Nonetheless, being responsible for the risks and sustainability of the organisation SAGE (2020:3), these leaders can not afford to neglect and delegate these high-risk functions and not participate in these discussions. Doing so will render them unaware of potential risks or opportunities and cause them to make decisions based on hearsay instead of first-hand quality information. The unawareness might harm the business and cause career damage to the leader, as found by Saban *et al.* (2021:278). These results coincide with those found by Naicker and Jairam-Owthar (2017:9), as discussed in the literature section.

The Q37 (11.2.2) results indicated high awareness and risk perception regarding PoPI Act. As such, the results from this study corroborate that of Saban *et al.* (2021:276), which found a positive correlation between the executives' (decision-makers) perception of security and external influencers like government regulations. The awareness and risk perception also increase. Thus, regulations significantly influence decision-makers to be more responsible. They are, therefore, more involved and tend to implement preventative actions. However, due to the enormous scope and constantly evolving cybersecurity landscape, SMEs require support from third parties like consultants, government agencies, and insurers to better manage the cybersecurity landscape, especially in building knowledge and increasing awareness (Hoppe *et al.*, 2021:254). Collaboration between these institutions will help improve cyber resilience and awareness at a national level, as PricewaterhouseCoopers (2018) suggests.

4.8 Hypothesis results

4.8.1 H1 result

H1: There is a positive relationship between decision-maker involvement in technology discussion and their perceived risk to the business.

1. The t-test correlation results between Q9 and Q29 indicate that decision-makers' perception changes towards the likelihood of an attack, and thus the risk to the business, only after a disaster occurs.
2. The practically significant correlation results of Q13 indicate an increased awareness of cyber risk to the business, positive impact of IT tools in the business, risk perception to the business and potential drivers for success depending on the involvement of the primary decision-makers.

3. The results for Q16 are troubling, considering that 39% of respondents leaned towards “always” delegating technology discussions to other employees.
4. As explained in the Q37 results, decision-makers seem more willing to get involved and stay updated with security aspects once regulatory institutions have coupled regulations and fines.

These results confirm the hypothesis that there is a positive relationship between decision-maker involvement and the perceived risks to the business.

4.8.2 H2 Results

H2: Increased technical understanding of the decision-maker positively correlates with the perceived risks of the business.

1. The practically significant correlation results of Q13 indicate an increased awareness of cyber risk to the business, positive impact of IT tools in the business, risk perception to the business and potential drivers for success depending on the involvement of the primary decision-makers.
2. The large, practically significant correlation results of Q14 (11.5.3) and Q19 against the risk perception questions show a positive correlation regarding technical understanding and perceived risk to the business.

The results also confirm the second hypothesis that increased technical understanding and inclination correlate with the perceived risk to the business.

4.8.3 H3 Results

There is a positive correlation between decision-maker involvement and technology adoption and integration into business strategy.

The practically significant correlation results of Q13 against Q21 (I am aware of the positive impact of IT tools and security on business competitiveness), Q28 (I Understand the impact IT tools and security have on business success.), Q30 (Indicate the level of risk to the business sustainability and competitive advantage if a cyber disaster event does occur), and Q35 (Technology adoption and innovation is a driver for business success in future) indicate a positive impact of IT tools in the business and potential

drivers for technology adoption success depending on the involvement of the primary decision-makers. Thus, the hypothesis is confirmed.

4.8.4 H0 Results

H0: There will be no difference in respondents' perceived risk to the business after the information session.

The H0 hypothesis is rejected in at least three questions, as there were practically visible increases:

1. The T-test and Wilcoxon rank test results for Q23 indicate a practically visible increase (effect = 0.32) in awareness of how vital IT tools and security are for a business.
2. Similarly, for Q29, the test indicates a practically visible difference (effect = 0.32) between the pre and post-test regarding the likelihood that the business will experience a cyber disaster event in the next year.
3. Finally, in Q32 regarding cybersecurity training as a priority in business, there was also a visible practical difference (effect = 0.39) between respondents' opinions before and after the information session. The results indicate that the priority regarding cybersecurity training increased after the information session.

4.9 Chapter conclusion

Chapter 4 analysed and discussed the data in detail. There were some worrying results described in the final discussion section 4.7 that SME decision-makers should urgently address. Finally, the researcher discussed whether the Hypotheses were accepted or rejected and provided examples and explanations. The next chapter will conclude the study with implications and recommendations.

CHAPTER 5: IMPLICATIONS AND LIMITATIONS

5.1 Chapter introduction

Much information exists in the news and internet about cybercrime statistics and the resultant costs and risks (Keeper, 2021:4-6). However, there is much less information in the context of these risks due to neglected leadership involvement. This chapter concludes with whether the study addressed the research questions and objectives. It further highlights implications to SMEs and provides recommendations to rectify the problems or mitigate the impact of security risks.

This study sought to investigate a relationship or correlation between leadership involvement in technical discussions and the related perception of security risk to the business. The literature section highlighted how vital technology and related security are to a business and how the separation of technology and business strategy is no longer an option. It further explored how perception can influence an organisation's culture and, as a result, influence the risks and potential opportunities of the organisation. Thus, from the literature, it is clear that awareness is critical for business leaders to change their perception and, therefore, their approach to incorporating technology into business management. If not aware of these risks, leaders will not adopt risk mitigation practices in the business, and even worse, not employing the available damage mitigation options through insurance products, as such will put the business at risk and not have the necessary protection in place when such a disaster does occur. The results from this study validate these problems to some extent.

5.2 Research questions and resolutions

Many questions did not show any significant correlation or effect size, which might be attributed to the study's small sample size (Maree, 2016:234). Nevertheless, the study results still indicated significant correlations in the relationship between leadership involvement and the leader's perceived risk to the business, which aligns with the study's primary objective. However, a larger sample would provide more clarity on the significance of the relationship. Additionally, to answer the research question, "does leadership involvement in technology discussions impact a leader's perceived risk to the business" the results show that it does.

5.3 Implications

The following section will discuss the implications of leaders and primary decision-makers do not change their behaviour and perception towards technology and cyber risks.

5.3.1 Involvement or participation

The results show that it is vital for leaders and primary decision-makers to be involved in every facet of technology and be more willing to understand, learn and read about the impact it has on business. Leaders can no longer separate technology from day-to-day business strategy, planning and decision-making, which should be integrated to understand technology's impact on business risks and opportunities. As Saban et al. (2021:278) highlight, leaders who do not change their attitude or behaviour accordingly might open the business to undue risk, limit potential growth, and soon be out of a job.

5.3.2 Awareness

The results show that increased awareness of the importance of information technology (Q23) and its implication on the business (Q29) will likely also increase the risk perception of respondents, at least increasing cybersecurity training (Q32), thus hopefully implementing preventative and mitigation options like obtaining insurance (Q34) against cybercrime. Only reacting after a loss event is not advisable and will result in unnecessary losses and damages to the SME and potential reputational damage (Keeper, 2021:4).

5.3.3 Culture

Being involved and thus more aware of the impact of information technology in the business will help leaders make better-informed decisions and achieve success. As the organisation's leaders, it is their responsibility to instil a culture of security awareness and integrate and adopt relevant technology in the business. An improved culture will undoubtedly improve business performance and help minimise risky employee actions and thus reduce the chance and scale of damage. On the other hand, it will also help leaders and employees to realise opportunities instead of just looking at these as grudge expenses.

5.4 Recommendations

1. The first recommendation is that SME leaders get involved in all technical discussions and read up on the impact of technology and the opportunities in the respective industries. Doing so will help leaders become more aware of risks and opportunities, but more importantly, they will be able to better convey the requirements and objectives of the organisation to the IT team or IT consultants.
2. Once the leader's awareness improves, they should create a security awareness and technology adoption culture to mitigate potential risks and utilise technology for operational and sustainable competitive advantages.
3. Lastly, within all business functions, technology and business strategy should be united to ensure proper workflow and operational efficiency and realise potential and improved competitive advantages from technology.

5.5 Limitations

Limitations of the study include the small number of respondents, although the researcher expanded the population and sample sizes to increase participation further. Another limitation is the measurement of the perception of decision-maker technology security and not the actual level of the security position of the company, which in itself can be a biased perception. Additionally, manipulating the variables through the presentation would depend on the participant watching the presentation, with little means of confirming if they watched the video in totality.

5.6 Future research

Future studies can investigate leadership involvement or participation in focus groups or specific businesses and business sectors.

Additional research could gauge the decision maker's perception of the company's security position against the reality through a third-party security assessment.

Another exciting study can test the significance and correlation of regulations on perceived risk and participation or involvement.

REFERENCES

- Abdulrahim, N. 2019. Managing Cybersecurity as a Business Risk in Information Technology-based Smes. University of Nairobi.
- Adams, R., Adeleke, F., Anderson, D., Bawa, A., Branson, N., Christoffels, A., ... Schonwetter, T. 2021. POPIA Code of Conduct for Research. South African Journal of Science, 117(5/6):20-31. 10.17159/sajs.2021/10933
- Al-rimy, B.A.S., Maarof, M.A. & Shaid, S.Z.M. 2018. Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions. Computers & Security, 74:144-166. <https://doi.org/10.1016/j.cose.2018.01.001>
- Alahmari, A. & Duncan, B. 2020. Cybersecurity Risk Management in Small and Medium-Sized Enterprises: A Systematic Review of Recent Evidence. pp. 1-5: IEEE.
- Artemenko, E. 2020. The roles of top management in digital transformation. IOP Conference Series: Materials Science and Engineering, 940(1):1-9.
- Astuti, E., Suhadak, Rahayu, S.M. & Wilopo. 2018. The influence of information technology strategy and management support to the internal business process, competitive advantage, financial and non-financial performance of the company. International Journal of Web Information Systems, 14(3):317-333. 10.1108/IJWIS-11-2017-0079
- Bada, M., Sasse, A.M. & Nurse, J.R. 2019. Cyber security awareness campaigns: Why do they fail to change behaviour? arXiv preprint arXiv:1901.02672,
- Bryman, A., Bell, E., Hirschsohn, P., dos Santos, A., du Toit, J. & Masenge, A. 2014. Research methodology: business and management contexts. 5th edition. Oxford University Press.
- Bughin, J., Catlin, T., Hirt, M. & Willmott, P. 2018. Why digital strategies fail. McKinsey Quarterly, 1:61-75.
- Choi, M. 2016. Leadership of Information Security Manager on the Effectiveness of Information Systems Security for Secure Sustainable Computing. Sustainability, 8(7):638. 10.3390/su8070638
- CSO. 2021. Global Intelligence Report: The State of Cybersecurity in 2021. <https://www.csoonline.com/resources/222430/global-intelligence-report-state-of-cybersecurity-2021> Date of access: 8 Aug. 2021.

de Koker, L.T. & du Plessis, T. 2020. Research as a service offering of knowledge management firms in the fourth industrial revolution. 2020, 22(1):1-8. 10.4102/sajim.v22i1.1178

Department of small business development. 2019. Revised Schedule 1 of the National Definition of Small Enterprise in South Africa. https://www.gov.za/sites/default/files/gcis_document/201903/423041gon399.pdf Date of access: 14 Oct. 2021.

Eling, M. & Schnell, W. 2016. What do we know about cyber risk and cyber risk insurance? *The Journal of Risk Finance*, 17(5):474-491. 10.1108/JRF-09-2016-0122

Field, A. 2009. *Discovering statistics using SPSS*. SAGE Publications Ltd.

Firstbrook, P., Olyaei, S., Shoard, P., Thielemann, K., Ruddy, M., Gaehtgens, F., ... Candrick, W. 2022. *Top Trends in Cybersecurity 2022*. <https://www.gartner.com/document/4011688?ref=solrAll&refval=335517795> Date of access:

Georgiadou, A., Mouzakitis, S., Bounas, K. & Askounis, D. 2020. A Cyber-Security Culture Framework for Assessing Organization Readiness. *Journal of Computer Information Systems*:1-11. 10.1080/08874417.2020.1845583

Gopal, N. & Maweni, V. 2019. Cybercrime Preparedness: A Critical Snapshot of BRICS Countries. *Africa Insight*, 49(2):70-88.

Hammarberg, R. & Gazzawi, A. 2022. *Risk Management Challenges For SMEs: A Case Study*.

Hodson, C.J. 2019. *Cyber risk management: Prioritize threats, identify vulnerabilities and apply controls*. Kogan Page Publishers.

Hoppe, F., Gatzert, N. & Gruner, P. 2021. Cyber risk management in SMEs: insights from industry surveys. *The Journal of Risk Finance*, 22(3/4):240-260. 10.1108/JRF-02-2020-0024

ISO, I.O.f.S. 2018. *ISO 31000:2018 Risk management — Guidelines*. Geneva, Switzerland: International Organization for Standardization. (ISO 31000:2018).

Jere, J.N. & Ngidi, N. 2020. A technology, organisation and environment framework analysis of information and communication technology adoption by small and medium enterprises in Pietermaritzburg. 2020, 22(1):1-9. 10.4102/sajim.v22i1.1166

Keeper. 2021. Ransomware impact report.

https://www.keeper.io/hubfs/2021_Ransomware_Impact_Report/2021_Ransomware_Impact_Report.pdf Date of access: 8 Aug. 2021.

Knapp, K.J., Marshall, T.E., Rainer, R.K. & Ford, F.N. 2006. Information security: management's effect on culture and policy. *Information Management & Computer Security*,

Lewis, B. & Kaiser, D. 2019. *There's No Such Thing As an IT Project : A Handbook for Intentional Business Change*. First Edition. Oakland, CA: Berrett-Koehler Publishers.

Maree, K. 2016. *First steps in research*. Second Edition. Van Schaik Publishers.

Marx, B. & Schutte, B. 2018. The role of information technology in the risk management of businesses in South Africa. *Journal for New Generation Sciences*, 16(2):92-111. 10.10520/EJC-151c33db08

Marx, D. 2017. The role of information technology (IT) in the risk management of businesses in South Africa.

Moufida, S., Steven, A. & Peter, B. 2020. It is not my job: exploring the disconnect between corporate security policies and actual security practices in SMEs. *Information & Computer Security*, 28(3):467-483. 10.1108/ICS-01-2019-0010

Moyo, M. & Loock, M. 2019. An Analysis of Small and Medium-Sized Enterprises' Perceptions of Security Evaluation in Cloud Business Intelligence. In. *International Conference on Cyber Warfare and Security*. Academic Conferences International Limited. pp. 554-XIII.

Mukhopadhyay, A., Chatterjee, S., Bagchi, K.K., Kirs, P.J. & Shukla, G.K. 2019. Cyber Risk Assessment and Mitigation (CRAM) Framework Using Logit and Probit Models for Cyber Insurance. *Information Systems Frontiers*, 21(5):997-1018. 10.1007/s10796-017-9808-5

Naicker, V. & Jairam-Owthar, D. 2017. The linkage of information quality to an executive decision support framework for the financial service sector of a developing economy. 2017, 19(1):1-9. 10.4102/sajim.v19i1.781

Nel, F. & Drevin, L. 2019. Key elements of an information security culture in organisations. *Information and Computer Security*, 27(2):146-164. 10.1108/ICS-12-2016-0095

- Okanga, B. 2017. Small- and medium-sized enterprises' knowledge management systems as edificers of new value innovations. 2017, 19(1):1-11.
10.4102/sajim.v19i1.786
- Olutoyin, O. & Flowerday, S. 2016. Successful IT governance in SMES: An application of the Technology–Organisation–Environment theory. 2016, 18(1):1-8.
10.4102/sajim.v18i1.696
- PricewaterhouseCoopers. 2018. The global state of information security survey 2018.
- Reynolds, S., Cotrino, F., Ifedi, C. & Donthu, N. 2020. An exploratory study of executive factors that lead to technology adoption in small businesses. *Journal of Small Business Strategy*, 30(2):1-16.
- Saban, K.A., Rau, S. & Wood, C.A. 2021. "SME executives' perceptions and the information security preparedness model". *Information & Computer Security*, 29(2):263-282. 10.1108/ICS-01-2020-0014
- SAGE. 2020. CFO 3.0 – Digital Transformation Beyond Financial Management.
<https://www.dailymaverick.co.za/wp-content/uploads/SA-CFO-3.0-Whitepaper-2020.pdf>
Date of access: 24 Aug. 2020.
- Saunders, M.N.K., Lewis, P. & Thornhill, A. 2019. *Research methods for business students*. Eighth edition. Pearson.
- Scholtz, T. 2019. Shift From Managing Risk and Security to Enabling Value Creation: The SRM Leaders' New Imperative. <https://www.gartner.com/en/doc/3913561-shift-from-managing-risk-and-security-to-enabling-value-creation> Date of access: 3 Apr. 2021.
- Schreckling, E. & Steiger, C. 2017. Digitalize or drown. In. *Shaping the digital enterprise*: Springer. pp. 3-27.
- Schutte, B. & Marx, B. The Role of Information Technology in the Risk Management of Businesses in South Africa.
- Sharma, S. & Aparicio, E. 2022. Organizational and team culture as antecedents of protection motivation among IT employees. *Computers & Security*, 120:102774.
<https://doi.org/10.1016/j.cose.2022.102774>
- Sibanda, M. & Ramrathan, D. 2017. Influence of information technology on organization strategy. *Foundations of Management*, 9(1):191-202.

Veiga, A., Looock, M. & Renaud, K. 2022. Cyber4Dev-Q: Calibrating cyber awareness in the developing country context. THE ELECTRONIC JOURNAL OF INFORMATION SYSTEMS IN DEVELOPING COUNTRIES, 88(1), 10.1002/isd2.12198

WEF. 2022. The Global Risks Report 2022.

https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf Date of access: 2 Aug. 2022.

Wilson, M. & Hash, J. 2003. Building an Information Technology Security Awareness and Training Program.

<https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-50.pdf> Date of access: 10 Aug. 2022.

Zhang, J. & Gopal, D. 2022. Hype Cycle for Cyber Risk Management, 2022: Gartner. <https://www.gartner.com/interactive/hc/4016974?ref=solrAll&refval=334411558>

ADDENDUM A: ETHICAL CLEARANCE



Private Bag X6001, Potchefstroom
South Africa 2520

Tel: 018 299-1111/2222
Web: <http://www.nwu.ac.za>

Economic and Management Sciences Research
Ethics Committee (EMS-REC)

2 November 2021

Dr K Ndlovu
Per e-mail
Dear Dr Ndlovu,

EMS-REC FEEDBACK: 29102021

Student: Pretorius, R (23345675)(NWU-001000-21-A4)

Study leader: Dr K Ndlovu - MBA

Your ethics application on, *Investigating involvement of leaders in technology discussions as mitigating factors of cyber risk in SMEs*, which served on the EMSREC meeting of 29 October 2021, refers.

Outcome:

Approved as a minimal risk study. A number **NWU-001000-21-A4** is given for one year of ethics clearance.

Please note that the ethics approval of this application is subject to the Covid-19 protocols.

Kind regards,

Prof Mark Rathbone

**Chairperson: Economic and Management Sciences Research Ethics Committee
(EMS-REC)**

ADDENDUM B: QUESTIONNAIRES, CONSENT FORMS AND INFORMATION SESSION

Pre-test

Online google questionnaire 1: <https://forms.gle/okP1nThtieg8D65s9>

Online information session 1: <https://youtu.be/z1y4IXK1cl8>

Post-test

Online google questionnaire 2: <https://forms.gle/o5aZ9DNRmNyCMzwQ8>

Online information session 2: <https://youtu.be/G9TCTG3jauw>

Consent form and questionnaire

The questionnaire below notes what the question attempts to test and includes the reference of where the question was previously used in research. The online google questionnaire was sent to participants as per the above links. The second questionnaire contained only the core questions from question 13 onwards to measure the correlations.

Research Questionnaire

You are herewith invited to participate in academic research with the below mentioned title. Participation is entirely voluntary and can be stopped at any time.

INFORMED CONSENT FOR PARTICIPATION IN ACADEMIC RESEARCH

Title: Investigating involvement of leaders in technology discussions as mitigating factors of cyber risk in SMEs.

Researcher: Mr Réno Pretorius (23345675) Email: reno@entrutech.co.za

Supervisor: Dr Kaizer Ndlovu email: 35181680@nwu.ac.za

Institution: North West University

Purpose of the study: The study aims to investigate the relationship between leadership involvement in technology discussion and the resulting perception of risk to the business. If required and on request, the researcher can provide a summary of the findings. Results of the study might be published in academic journals. No identifiable information will be presented in the final publication.

Expectations: Please read through this consent form to familiarise yourself with your rights and expectations for participating in this study.

Confidentiality: All information obtained and analysed during this study is purely for academic purposes with no intentions of sharing and making it public and will be treated as confidential. The data and resultant report will be stored in a secure encrypted environment and kept at the North West University for a maximum of 5 years.

Research procedures: Participants will be required to complete a questionnaire (8-10 Minutes), after which an online informational video (10 Minutes) will be available to watch. The video will highlight associated technical risks to SMEs and leaders themselves. 3 Days later, respondents will complete only the primary questions of the questionnaire again (8 minutes) to determine the difference in risk perception. After the second questionnaire another short video session will be available to highlight practical mitigation strategies, tools and recommendations participants can use.

Incentives: Additional to the information session, you are eligible for a free online business risk assessment as a token of appreciation for your participation.

Your rights: Your participation in this study is vital. However, you may choose not to participate or stop partaking at any time without having to state a reason or any negative consequences. As a participant, you are welcome to contact the Researcher at any time to highlight ethical concerns or other issues relating to this study. If the option is selected, a copy of this electronic approved consent form will be sent to you.

Data analysis: data will be analysed by experts at the North-West University Statistical Consultation Service with appropriate statistical software.

Duration of the study: The study will be conducted over a total period of 10 months.

If you have any questions or concerns during or after the interview, kindly contact **Réno Pretorius** or Dr **Kaizer Ndlovu** with the above-listed contact details.

Your data will not be used for any other research unless approved by you. Any ethical concerns may be directed to the Universities ethics committee.

1. I hereby confirm that I have been informed about the nature of this research and understand my rights.

I accept participation in this study?

Mark only one oval.

☐ Yes

Section 2

2. **Email address as unique identifier:** *

Please enter your email address as unique identifier and for the follow up questionnaire within 3 days (shorter). Your email address will not be shared or used for any other purpose.

Demographic information

3. Age Group

☐ <20	☐ 21-30	☐ 31-40	☐ 41-50	☐ 51-60	☐ 60+
------------------------------	--------------------------------	--------------------------------	--------------------------------	--------------------------------	------------------------------

4. Position or affiliation at the business

- a. ☐ Manager
- b. ☐ C level or director
- c. ☐

5. Highest academic qualification

- a. ☐ Higher Certificate
- b. ☐ National Diploma
- c. ☐ Bachelor's Degree
- d. ☐ Honours Degree
- e. ☐ Master's Degree or higher

6. The number of permanent employees, using computers daily, in the business.

☐ <5	☐ 6-10	☐ 11-20	☐ 20-40	☐ 50-100	☐ 100-250
-----------------------------	-------------------------------	--------------------------------	--------------------------------	---------------------------------	----------------------------------

7. Age of the business

☐ <3 years	☐ 3-5 years	☐ 6-10 years	☐ 11-20 years	☐ 20+ years
--------------------------------------	---------------------------------------	--	---	---------------------------------------

Questions

8. Are you the primary decision-maker with regard to technology adoption in your organisation?

- ☐ Yes
- ☐ An influencer to the primary decision-maker
- ☐ No

Business Background

9. Our business experienced one or more cyber attacks or ransomware before.

- ☐ Yes
- ☐ No

10. My organisation has an information security policy in place, also referred to as an Acceptable Usage Policy. Adapted from ISCA, question 2, Da Veiga (2018)

- ☐ Yes
- ☐ No

11. Is the business registered with the Potchefstroom Chamber of Commerce or ProPotch initiative.

- ☐ Yes

☐ No

12. If yes, please name Chamber and / or initiative for relevance in this study.

Please rate the level of involvement in the following scenarios:

13. Primary technology decision-makers are always involved in technical discussions with the IT team or contractor about technology and related security for the business. (*involvement in technology discussions*)

Never	☐	☐	☐	☐	☐	☐	☐	Always
-------	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	--------

14. Interested in security issues and mitigation options – adapted from (Knapp, Marshall, Rainer & Ford, 2006) (technical knowledge and inclination to be involved)

Low	☐	☐	☐	☐	☐	☐	☐	High
-----	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	------

15. Consider IT tools and security an essential organisational priority. (*Inclination to be Involvement*). Adapted from (Knapp *et al.*, 2006)

Low	☐	☐	☐	☐	☐	☐	☐	High
-----	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	------

16. I do not attend technology discussions. The jargon/tech language frustrates me. (*Involvement*)

Low	☐	☐	☐	☐	☐	☐	☐	High
-----	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	------

17. Take IT tools and security into account when planning business strategies. (*Inclination to be Involvement*) - adapted from (Knapp *et al.*, 2006)

Never	☐	☐	☐	☐	☐	☐	☐	Always
-------	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	--------

18. Regularly attend webinars or seminars about technology risks to businesses.
(technical understanding and inclination to attend discussions)

Low	☐	☐	☐	☐	☐	☐	☐	High
-----	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	------

19. Regularly read about technology and cyber security risks to the business.
(technical understanding and inclination to attend discussions)

Low	☐	☐	☐	☐	☐	☐	☐	High
-----	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	------

20. Aware of technical challenges experienced by employees and how to improve.
(Awareness of IT impact on business)

Low	☐	☐	☐	☐	☐	☐	☐	High
-----	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	------

21. Aware of the positive impact of IT tools and security on business competitiveness.
(Awareness of IT impact on business)

Low	☐	☐	☐	☐	☐	☐	☐	High
-----	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	------

Risk perception to business

Please rate the level of perception on the following statements:

21. Technology security and cyber-attacks pose a significant risk to the business. (Risk perception)

Low	☐	☐	☐	☐	☐	☐	☐	High
-----	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	------

22. IT tools and security is a waste of money as protection can not be 100% secure
(IT adoption tendency)

Low	☐	☐	☐	☐	☐	☐	☐	High
-----	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	------

23. **How concerned is the organisation about IT and cyber security?** (risk perception) From (Abdulrahim, 2019:67)

Low	☐	☐	☐	☐	☐	☐	☐	High
-----	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	------

24. Technology and related security is merely an expense item. (*perception towards IT*)

Low	☐	☐	☐	☐	☐	☐	☐	High
-----	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	------

25. How much of a risk is cybercrime to the business. (*Risk perception*)

Low	☐	☐	☐	☐	☐	☐	☐	High
-----	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	------

26. How much of a risk is cybercrime to yourself. (*Risk perception*)

Low	☐	☐	☐	☐	☐	☐	☐	High
-----	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	------

27. **Understand the impact IT tools and security has on business success.** (IT adoption tendency). Adapted from (Choi, 2016).

Low	☐	☐	☐	☐	☐	☐	☐	High
-----	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	------

28. Indicate the likeliness that the business will experience a cyber disaster event in the next year (Ransomware, cyber attack, virus). (*Risk Perception*)

Low	☐	☐	☐	☐	☐	☐	☐	High
-----	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	------

29. Level of risk to the business sustainability and competitive advantage if such an event does occur. (*Risk perception*)

Low	☐	☐	☐	☐	☐	☐	☐	High
-----	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	------

30. The business is sufficiently prepared for a total data loss disaster event like ransomware, theft, fire. (*Risk Perception*)

Low	☐	☐	☐	☐	☐	☐	☐	High
-----	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	------

31. **Is cybersecurity training a priority in the business?** (*Risk awareness*). Adapted From (Abdulrahim, 2019:67)

Low	☐	☐	☐	☐	☐	☐	☐	High
-----	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	------

32. **Have an IT security policy and recovery plan in place and is updated regularly?** (*IT adoption and Preparedness*). Adapted from (Knapp et al., 2006)

Low	☐	☐	☐	☐	☐	☐	☐	High
-----	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	------

33. Aware of insurance products against potential losses of data or cyber-attacks. (*Awareness of risk mitigation options*)

Low	☐	☐	☐	☐	☐	☐	☐	High
-----	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	------

34. Fully aware of PoPI Act and related technology requirements and fines. (*Risk perception*)

Low	☐	☐	☐	☐	☐	☐	☐	High
-----	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	------

35. Technology adoption and innovation is a driver for business success in future. (*IT adoption tendency*)

Low	☐	☐	☐	☐	☐	☐	☐	High
-----	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	------

36. Technology security is a foundation for businesses to be PoPI Act compliant. (*Risk perception*)

Low	☐	☐	☐	☐	☐	☐	☐	High
-----	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	------

ADDENDUM C: LANGUAGE EDITOR CERTIFICATE



30 November 2022
Pretoria, South Africa

To whom it may concern,

I hereby confirm that I undertook the language editing for the MBA dissertation:

Investigating the involvement of leaders in technology discussions as mitigating factors of cyber risk in SMEs

by Reno Pretorius, student no. 23345675

Cillié Swart BA (Harvard) MBA (Kuehne)
+27 (0)73 612 0278
pjcswart@transkaroo.net

ADDENDUM D: SIMILARITY INDEX

23345675:Pretorius-R-23345675-MBAC-873-
Dissertation_REV_2.docx

ORIGINALITY REPORT

10 %	9 %	2 %	3 %
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	dspace.nwu.ac.za Internet Source	1 %
2	repository.nwu.ac.za Internet Source	1 %
3	Submitted to North West University Student Paper	<1 %
4	repository.up.ac.za Internet Source	<1 %
5	docs.google.com Internet Source	<1 %
6	core.ac.uk Internet Source	<1 %
7	hdl.handle.net Internet Source	<1 %
8	igemiracle.weebly.com Internet Source	<1 %
9	Submitted to Royal Holloway and Bedford New College	<1 %

ADDENDUM E: DESCRIPTIVE STATISTICS

Descriptive Statistics					
Question number	N	Minimum	Maximum	Mean	Std. Deviation
Q13	36	1	7	5.69	1.79
Q14	36	1	7	5.14	1.61
Q15	36	1	7	6.08	1.44
Q16	36	1	7	3.69	2.00
Q17	36	1	7	5.36	1.79
Q18	36	1	7	3.03	1.93
Q19	36	1	7	3.58	1.87
Q20	36	1	7	4.75	1.79
Q21	36	1	7	5.44	1.90
Q22	36	1	7	5.28	2.19
Q23	36	1	6	2.11	1.39
Q24	36	1	7	5.22	1.97
Q25	36	1	7	2.50	1.80
Q26	36	1	7	4.94	1.91
Q27	36	1	7	4.78	1.96
Q28	36	1	7	5.50	1.76
Q29	36	1	7	2.94	1.64
Q30	36	1	7	4.92	2.20
Q31	36	1	7	4.44	2.03
Q32	36	1	7	3.72	1.86
Q33	36	1	7	4.31	1.91
Q34	36	1	7	3.86	2.13
Q35	36	1	7	5.31	1.82
Q36	36	1	7	5.81	1.62
Q37	36	3	7	5.94	1.26
Q14_Post	16	1	7	4.88	1.78
Q15_Post	16	5	7	6.13	0.89
Q16_Post	16	2	7	3.94	1.91
Q17_Post	16	3	7	5.50	1.15
Q21_Post	16	2	7	5.94	1.39

Q22_Post	16	3	7	5.63	1.36
Q23_Post	16	1	4	1.88	0.89
Q14_Post2	16	2	7	5.31	1.30
Q25_Post	16	1	5	2.13	1.02
Q26_Post	16	2	7	5.19	2.07
Q27_Post	16	2	7	4.81	1.91
Q28_Post	16	4	7	5.94	0.85
Q29_Post	16	1	6	3.81	1.80
Q30_Post	16	1	7	5.50	1.51
Q31_Post	16	1	7	4.56	1.82
Q32_Post	16	1	7	4.06	1.95
Q34_Post	16	1	6	4.25	1.48
Q35_Post	16	1	7	5.25	1.98
Q37_Post	16	3	7	6.06	1.12
Valid N (listwise)	16				