

https://dspace.org/

Investigating cyber resilience in Small, Medium, and Micro Enterprises (SMME's) in Gauteng

Kamanga, Edna Clara

2022
University of the Witwatersrand, Johannesburg
https://hdl.handle.net/10539/44238
Kamanga, Edna Clara. (2022). Investigating cyber resilience in Small, Medium, and Micro Enterprises (SMME's) in Gauteng [Master's dissertation, University of the Witwatersrand, Johannesburg].WireDSpace.

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

Investigating cyber resilience in Small, Medium, and Micro Enterprises (SMME's) in Gauteng

Edna Clara Kamanga

2417875@students.wits.ac.za

A research proposal submitted to the Faculty of Commerce, Law, and Management, University of the Witwatersrand, in partial fulfilment of the requirements for the degree of Master of Management in the field of Digital Business

Johannesburg, 2022

KEYWORDS

Cyber resilience, Cyber risk, Critical Information systems, NIST Framework, Critical Success Factors, Small, Micro, Medium Enterprises, Cyber Security Frameworks, Cybersecurity, Cyber-attacks, cyber threats

TABLE OF CONTENTS

ABSTRACT ..... **vi**

DEDICATION ..... **vii**

ACKNOWLEDGEMENT ..... **viii**

LIST OF TABLES ..... **ix**

LIST OF FIGURES ..... **x**

LIST OF ACRONYMS ..... **xiii**

CHAPTER 1. INTRODUCTION **14**

1.1 STATEMENT OF PURPOSE 14
1.2 BACKGROUND OF THE STUDY 14
1.3 RESEARCH PROBLEM 16
1.4 RESEARCH QUESTION 17
1.5 RATIONALE OF THE STUDY 17
1.6 DELIMITATIONS OF THE STUDY 18
1.7 ETHICAL CONSIDERATION 19
1.8 DEFINITION OF TERMS 19
1.9 ASSUMPTIONS 21
1.10 CHAPTER OUTLINE 22

CHAPTER 2.LITERATURE REVIEW AND THEORETICAL FRAMEWORK **24**

2.1 INTRODUCTION 24
2.2 CYBERSPACE CHALLENGES AMONG SMMES 25
2.3 CYBER RESILIENCE 27
2.4 IMPORTANCE OF CYBER RESILIENCE 29
2.5 CYBER RESILIENCE FRAMEWORKS 30
2.6 ASSESSING CRITICAL SUCCESS FACTOR PRACTICES IMPLEMENTED 33
2.7 CYBER RESILIENCE CRITICAL SUCCESS FACTORS 35
2.7.1 CYBERSECURITY AWARENESS AND TRAINING 35
2.7.2 RISK ASSESSMENT AND MANAGEMENT 35
2.7.3 INCIDENT RESPONSE AND BUSINESS CONTINUITY 36
2.7.4 ACCESS CONTROL AND PRIVILEGE MANAGEMENT 36
2.7.5 NETWORK AND PERIMETER SECURITY 37
2.7.6 PATCH MANAGEMENT 37
2.7.7 DATA BACKUP AND RECOVERY 38
2.7.8 VENDOR AND THIRD-PARTY MANAGEMENT 38

2.7.9 Continuous Monitoring and Threat Intelligence 38
2.3.10 Cyber resilience critical success factors conclusion 39
2.8 Measuring critical success factors to cyber resilience. 39

CHAPTER 3.RESEARCH METHODOLOGY 40

3.1 Introduction 40
3.2 Philosophical Underpinnings and Research Paradigms 40
3.3 Research Design 42
3.4 Research Approach 43
3.5 Sampling: Design and Procedures 44
3.5.1 Target Population 44
3.5.2 Sampling Frame 44
3.5.3 Sampling techniques 44
3.5.4 Sample Size 45
3.5.5 Critical Success Factors and Best Practices: 46
3.5.6 Develop Research Framework: 46
3.6 Data Collection 47
3.6.1 Interview Guide 47
3.6.2 Data Collection: 48
3.6.3 Data Analysis: 49
3.7 Possible Limitations and Challenges of the Study 49
3.8 Quality Assurance 50
3.8.1 External Validity or Transferability 50
3.8.2 Internal Validity OR Credibility 51
3.8.3 Reliability OR Dependability 51

CHAPTER 4. ..... RESULTS 54

4.1 Introduction 54
4.2 Findings 55
4.3 How do SMMEs in Gauteng anticipate, detect, withstand, and recover from cyber incidents? 56
4.3.1 Ability to Identify, Detect, Protect, Recover, and Respond 58
4.4 Do SMMEs in Gauteng implement the different dimensions of cyber resilience framework? 59
4.5 What are the key success factors or best practices that demonstrate the cyber resilience of critical information systems among SMMEs in Gauteng? 60
4.6 Conclusion on Findings 61

CHAPTER 5.CONCLUSION AND RECOMMENDATION 63

5.1 Introduction 63

5.2 How do SMMEs Approach Cyber Resilience 64
5.3 Do SMMEs in Gauteng employ all the dimensions of the CR-SAT framework..... 65
5.4 What are key critical success factors for SMME in Gauteng. 65
5.5 Conclusion and recommendations 66

APPENDIX A – Research Instrument.....74

APPENDIX B – Participant Information 76

APPENDIX C – Participant Consent Form.....79

APPENDIX D – Signed Non-Disclosure Agreement.....81

APPENDIX E – Supervisor Email 84

ABSTRACT

Title: Investigating Cyber Resilience, in Small, Medium, and Micro Enterprises (SMMEs) in Gauteng: A Qualitative Inquiry

Abstract:

Cyber resilience is becoming increasingly vital for Small, Medium, and Micro Enterprises (SMMEs) to withstand and quickly recover from cyber threats. This qualitative study investigates the cyber resilience strategies, critical success factors, and best practices within SMMEs in Gauteng, South Africa. The research aims to understand SMMEs approach to cyber resilience and whether they incorporate all dimensions of the Cyber Resilience-Self Assessment Tool (CR-SAT), a framework specifically recommended for enhancing the cyber resilience of SMMEs. The study identifies key critical success factors that are prevalent among Gauteng's SMMEs.

The methodology involves semi-structured interviews with business owners, IT Managers, and cybersecurity experts within a variety of SMMEs in Gauteng. The selection of participants ensures representation across different industries to allow for comprehensive insights into the cyber resilience landscape within this economic sector. Thematic analysis of the interview data provides an in-depth understanding of the experiences, practices, and perceptions of cyber resilience among participants.

Preliminary findings reveal that while some SMMEs demonstrate awareness and implementation of cyber resilience best practices, there is a varied degree of adoption concerning the CR-SAT framework. Several critical success factors emerge, these include adoption of best practices in implementation of training and awareness, risk management, business continuity, the implementation of incident response plans, outsourcing, dealing with credible vendors. However, the research also identifies significant gaps in knowledge and resource constraints, which impede full-scale implementation of recommended cyber resilience measures.

DEDICATION

To my late mother and father who have gone before me I salute your greatness. Thank you for setting the standard for your children, your legacy will live on through our generation.

ACKNOWLEDGEMENT

Thank you, Dr Kiru Pillay, for your support throughout this study. To my employer, thank you for affording me the opportunity to dream bigger. To my family, thank you for allowing me to the time to focus and study.

LIST OF TABLES

Table 1: Characteristics of Cybersecurity vs. Cyber resilience..... 29

Table 2: Measuring cyber resilience, scale rating and moderated descriptors Carias, *et a*l. (2021)..... 34

Table 3: Categories of Scientific paradigms and their classifications..... 42

Table 4: Key Dimensions Result Findings..... 57

Table 5: Detailed Dimensions Moderated Scale Score Finding**s** 58

LIST OF FIGURES

Figure 1: Theoretical Framework adapted from NIST Framework 33

Figure 2: Research Framework..... 47

Figure 3: Key Dominant Critical Success Factors for SMMEs in Gauteng 60

Contents

ABSTRACT vi

DEDICATION vii

ACKNOWLEDGEMENT viii

LIST OF TABLES ix

LIST OF FIGURES x

LIST OF ACRONYMS xiii

CHAPTER 1. ..... INTRODUCTION 14

1.1 STATEMENT OF PURPOSE 14
1.2 BACKGROUND OF THE STUDY 14
1.3 RESEARCH PROBLEM 16
1.4 RESEARCH QUESTION 17
1.5 RATIONALE OF THE STUDY 17
1.6 DELIMITATIONS OF THE STUDY 18
1.7 ETHICAL CONSIDERATION 19
1.8 DEFINITION OF TERMS 19
1.9 ASSUMPTIONS 21
1.10 CHAPTER OUTLINE 22

CHAPTER 2.LITERATURE REVIEW AND THEORETICAL FRAMEWORK 24

2.1 INTRODUCTION 24
2.2 CYBERSPACE CHALLENGES AMONG SMMES 25
2.3 CYBER RESILIENCE 27
2.4 IMPORTANCE OF CYBER RESILIENCE 29
2.5 CYBER RESILIENCE FRAMEWORKS 30
2.6 ASSESSING CRITICAL SUCCESS FACTOR PRACTICES IMPLEMENTED 33
2.7 CYBER RESILIENCE CRITICAL SUCCESS FACTORS 35
2.7.1 CYBERSECURITY AWARENESS AND TRAINING 35
2.7.2 RISK ASSESSMENT AND MANAGEMENT 35
2.7.3 INCIDENT RESPONSE AND BUSINESS CONTINUITY 36
2.7.4 ACCESS CONTROL AND PRIVILEGE MANAGEMENT 36
2.7.5 NETWORK AND PERIMETER SECURITY 37
2.7.6 PATCH MANAGEMENT 37
2.7.7 DATA BACKUP AND RECOVERY 38
2.7.8 VENDOR AND THIRD-PARTY MANAGEMENT 38
2.7.9 CONTINUOUS MONITORING AND THREAT INTELLIGENCE 38
2.3.10 CYBER RESILIENCE CRITICAL SUCCESS FACTORS CONCLUSION 39
2.8 MEASURING CRITICAL SUCCESS FACTORS TO CYBER RESILIENCE. 39

CHAPTER 3.RESEARCH METHODOLOGY 40

3.1 INTRODUCTION 40
3.2 PHILOSOPHICAL UNDERPINNINGS AND RESEARCH PARADIGMS 40
3.3 RESEARCH DESIGN 42
3.4 RESEARCH APPROACH 43
3.5 SAMPLING: DESIGN AND PROCEDURES 44
3.5.1 TARGET POPULATION 44
3.5.2 SAMPLING FRAME 44
3.5.3 SAMPLING TECHNIQUES 44
3.5.4 SAMPLE SIZE 45
3.5.5 CRITICAL SUCCESS FACTORS AND BEST PRACTICES: 46
3.5.6 DEVELOP RESEARCH FRAMEWORK: 46
3.6 DATA COLLECTION 47
3.6.1 INTERVIEW GUIDE 47
3.6.2 DATA COLLECTION: 48
3.6.3 DATA ANALYSIS: 49
3.7 POSSIBLE LIMITATIONS AND CHALLENGES OF THE STUDY 49
3.8 QUALITY ASSURANCE 50
3.8.1 EXTERNAL VALIDITY OR TRANSFERABILITY 50
3.8.2 INTERNAL VALIDITY OR CREDIBILITY 51
3.8.3 RELIABILITY OR DEPENDABILITY 51

CHAPTER 4. RESULTS 54

4.1 INTRODUCTION 54
4.2 FINDINGS 55
4.3 HOW DO SMMES IN GAUTENG ANTICIPATE, DETECT, WITHSTAND, AND RECOVER FROM CYBER INCIDENTS? 56
4.3.1 ABILITY TO IDENTIFY, DETECT, PROTECT, RECOVER, AND RESPOND 58
4.4 DO SMMES IN GAUTENG IMPLEMENT THE DIFFERENT DIMENSIONS OF CYBER RESILIENCE FRAMEWORK? 59
4.5 WHAT ARE THE KEY SUCCESS FACTORS OR BEST PRACTICES THAT DEMONSTRATE THE CYBER RESILIENCE OF CRITICAL INFORMATION SYSTEMS AMONG SMMES IN GAUTENG? 60
4.6 CONCLUSION ON FINDINGS 61

CHAPTER 5.CONCLUSION AND RECOMMENDATION 63

5.1 INTRODUCTION 63
5.2 MEASURING CYBER RESILIENCE USING THE MODERATED SCALE SCORE RATING 63
5.3 HOW DO SMMES APPROACH CYBER RESILIENCE 64
5.4 DO SMMES IN GAUTENG EMPLOY ALL THE DIMENSIONS OF THE CR-SAT FRAMEWORK 65
5.5 WHAT ARE KEY CRITICAL SUCCESS FACTORS FOR SMME IN GAUTENG. 65
5.6 CONCLUSION AND RECOMMENDATIONS 66

APPENDIX A – Research Instrument 74

APPENDIX B – Participant Information 76

APPENDIX C – Participant Consent Form 79

APPENDIX D – Signed Non-Disclosure Agreement 81

APPENDIX E – Supervisor Email 84

LIST OF ACRONYMS

CRMM – Cybersecurity Resilience Maturity Measurement

CIS – Critical Information Systems

CSF – Critical Success Factors

SMME – Small Micro Medium Enterprise

Put these into alphabetical order.

CHAPTER 1. INTRODUCTION

1.1 Statement of purpose

This research explores cyber resilience (CR) in Small, Medium, and Micro Enterprises (SMMEs) in Gauteng. The study involves researching cyber resilience critical success factors and best practices that are exhibited in SMMEs for their critical information systems (CIS).

1.2 Background of the study

The National Development Plan (NDP) outlines various objectives for South Africa by the year 2030, encompassing the eradication of poverty, mitigation of inequality, and achieving a target unemployment rate of six percent. Bridging this considerable gap between the envisaged goals and the present economic conditions poses a significant challenge for the country. While reporting a per-capita expenditure Gini coefficient of 0,67 in 2006 and dropping to 0,65 in 2015 (Stats_SA, 2022) South Africa is labelled as one of the most unequal countries in the world. This calls for significant attention to be drawn to the acceleration of innovative ways that allow for inclusive growth to eliminate poverty, inequality, and unemployment.

SMMEs have been recognised as a crucial contributor to employment and economic growth in South Africa since 1994 (Agupusi, 2007). In recent years, there has been a renewed focus on the promotion of SMMEs due to the rise in unemployment, with both the government and private sector emphasizing their importance in job creation and poverty reduction, particularly among historically disadvantaged groups (Vuba, 2019). According to an article by Business-Tech, SMMEs in South Africa are responsible for creating 4.8 million jobs, which is equivalent to 60% of the country's employment (Bhorat *et al.*, 2018). Similarly, (Cheung, 2017) notes that SMMEs contribute approximately 42% to South Africa's gross domestic product (GDP) and account for about 60% of employment, representing over 90% of formal businesses. Accordingly, active SMMEs are not only crucial for driving productivity and growth (Rungani *et al.*,

2018), but also are instrumental in reducing poverty and the unemployment rate (Bvuma & Marnewick, 2020) in the country.

Despite the significant role they play, SMMEs are faced with numerous challenges such as, access to finance, markets, and skills development, as well as poor infrastructure, and inefficient bureaucracy. Since 2019, when the COVID-19 pandemic hit our shores in South Africa, many businesses have had to operate on various digital platforms to extend their market by reaching a greater number of customers (Gabriel *et al.*, 2021). This exposure to the digital world has brought about further challenges to the already ailing business landscape, particularly for those who are unfamiliar with cybersecurity best practices. Studies conducted by (Carías *et al.*, 2020) show that SMMEs face several challenges when it comes to cybersecurity, including budget constraints, lack of employees with cybersecurity skills, management support, and commitment toward cybersecurity concerns in IT systems. These challenges make it difficult for SMMEs to implement effective cybersecurity measures and to protect their critical information systems from potential cyber threats thereby, leaving SMMEs systems vulnerable to cyber-attacks due to inadequate cybersecurity protection.

The cyberthreat landscape is constantly evolving and is becoming of great concern for management Carías *et al*., (2020). A recent study by (Jovanovic, 2024; Robert P. Hartwig & Claire, 2013) highlights a few statistics in relation to cybercrime. Studies highlight that 560,000 new pieces of malware are detected every day; more than one billion malware programs exist; four companies fall victim to ransomware attacks every minute; and Trojans account make up 58% of all computer malware. Additionally, in a report on cybercrime (Robert Johnson, 2019) noted that 60 percent of small companies go out of business within six months after falling victim to a data breach or cyberattack. Furthermore, a research conducted by (IBM, 2022) highlighted that, ransomware, phishing, email spoofing, and data breach costs have the potential to erode the benefits of the digital economy by increasing operational cost and reduced operational efficiency of the SMMEs (Hills & Atkinson, 2016), (NIST, 2018). Cyber-attacks can be carried out through various threat vectors such as distributed denial-of-service (DDoS) attacks, phishing attempts, malware campaigns, ransomware attacks,

and other malicious activities that can negatively impact the operation of the organization through increased cyber-risk (Chatterjee, 2020). However, as highlighted above the landscape of these threat vectors continues to grow. Accordingly, this study explored the critical success factors that influence the cyber resilience of critical information systems of SMMEs, the extent to which these factors are exhibited among SMMEs in Gauteng.

1.3 Research Problem

SMMEs are increasingly reliant upon complex and interconnected cyber systems to conduct daily operations and deliver on their organisational goals and objectives. From utilising digital assets for critical operational activities like e-commerce to controlling a vast web of digitized information systems (Lang & Li, 2013). While the increasing interconnectivity of systems has undoubtedly brought about significant improvements in service delivery efficiency, it has also exposed users to unintended consequences in the form of cyber threats from attackers (Umunnakwe *et al.*, 2021). Unlike larger organizations, SMMEs often lack the capacity and resources to implement robust cybersecurity measures and are, therefore, more likely to suffer from cyber breaches. This can result in significant losses, which can erode the welfare of the South African economy and its people (Solms, 2019).

The academic literature has increasingly focused on the management of cyber resilience among SMMEs, highlighting the significance of this economic endeavour. Several recent studies have explored the impact of cybercrime on SMMEs and the need for a specific cyber resilience framework oriented for SMMEs. For example, a literature review on cyber resilience frameworks emphasized the lack of frameworks designed specifically for SMMEs, as existing frameworks often include policies that might not be applicable to SMMEs (Carías *et al.*, 2020) Additionally, a self-assessment tool for cyber resilience in SMMEs has been proposed, indicating a growing interest in providing practical resources for SMMEs to enhance their cyber resilience (Carias *et al.*, 2021) Despite these efforts, there remains a research gap in identifying a comprehensive and tailored cyber resilience framework for SMMEs, considering their unique resource

constraints and risk profiles. Further research is needed to evaluate the critical success factors best practices that can help SMMEs reduce cyber related risks.

1.4 Research Question

This study entails to address the following research questions:

Research Question

This study entails to address the following research questions:

- How do SMMEs in Gauteng anticipate, detect, withstand, and recover from cyber incidents?
- Which key dimensions of a cyber resilience framework are implemented by SMMEs?
- What are the key success factors or best practices that demonstrate the cyber resilience of critical information systems among SMMEs in Gauteng?

Based on the research questions the following research objectives are derived:

- To what approach to cyber resilience is employed by the SMMEs in Gauteng anticipate, detect, withstand, and recover from cyber incidents.
- To explore to what extent the practices, procedures of the 11 essential dimensions as recommended in the CR-SAT theoretical framework are employed by the SMME.
- To establish which of the 11 essential dimensions are key to SMMEs in Gauteng.

1.5 Rationale of the study

The rationale for conducting research on the cyber resilience of Critical Information Systems of SMMEs in Gauteng is multifaceted. Research shows that that a significant percentage of SMMEs, including those in South Africa, have experienced cyber security incidents, indicating the vulnerability of these

businesses to cyber threats (Caitlyn Murphy *et al.*, 2022). Additionally, the Gauteng Department of e-Government has emphasized the importance of cyber security through its Strategic Plan, further underscoring the significance of this research within the local context. Furthermore, the increasing reliance of SMMEs on technological advancements and the need for compliance with national cyber security policies highlight the critical nature of ensuring the cyber resilience of their information systems. Given these factors, it is imperative to explore how cyber resilience strategies translate to the specific context of SMMEs in Gauteng. This knowledge can inform strategies for fostering a cybersecurity culture within SMMEs and promoting the integration of cyber resilience practices into their day-to-day operations. And thereby, help SMMEs make informed decisions about which strategies are most effective in protecting their critical information systems.

1.6 Delimitations of the study

This study focussed on evaluating the critical success factors that influence cyber resilience of SMMEs of their critical information systems. The extent to which the critical success factors are exhibited in the SMME. This study was be limited to the criteria below.

1. **SMMEs** as defined by in The National Small Business (NSB) Act of South Africa (Africa, 1996)
2. **Geographic scope:** included SMMEs in Gauteng
3. **Industry focus:** The study focused on SMMEs that use digital technologies as part of their operational strategy, excluding SMMEs dealing in the health and education sectors.
4. **Size of SMMEs:** The study could focus on SMMEs that have between 1 to not greater than 200 employees, a turnover of R200 000 to R50m and assets value of less than R100 000 to R18m. SMMEs as defined by the National Small Business Act of South Africa.
5. **Methodology:** The study used qualitative research methodology, to collect data using open ended interview questions.

1.7 Ethical Consideration

Ethical consideration included the following:

- Obtain informed consent from participants, ensuring they have a clear understanding of the research purpose.
- Safeguard the privacy and confidentiality of participants.
- Implement appropriate measures to protect the security and integrity of participants' data. Consider various laws including POPIA.
- Treat participants with respect, dignity, and fairness.
- Be transparent and honest with participants about the purpose and nature of the research.
- Seek ethical approval from WITS ethics committees before conducting the research.
- Transparency and reporting report the research methods, procedures, and findings in a transparent and accurate manner.

1.8 Definition of terms

The following list key words and concepts used in this research proposal document:

Term	Description
Cyber resilience	is the ability to continuously deliver the intended outcome despite adverse cyber events (Björck *et al.*, 2015). The capacity to withstand, recover from, and adapt to the external shocks caused by cyber risks (Dupont, 2019)
Cyber Risk	is the potential harm or damage that can result from a cyberattack or other type of cyber threat. It encompasses a wide range of risks, including financial losses, reputational damage, legal liabilities, and operational disruptions. Cyber risk can arise from a variety of sources, including malicious actors seeking to steal sensitive data or disrupt operations, accidental or unintentional actions by employees or other insiders, and technical failures or vulnerabilities in hardware or software systems. Effective cybersecurity measures are essential for managing cyber risk and minimizing the potential impact of cyber threats on an organization's operations and reputation (NIST, 2018), (Radanliev *et al.*, 2019).
Cybersecurity	is the practice of protecting computer systems, networks, and digital information from unauthorized access, theft, damage, or other malicious attacks. It involves a range of technologies, processes, and practices designed to safeguard devices, data, and networks from cyber threats such as viruses, malware, phishing attacks, hacking attempts, and other forms of cybercrime. Cybersecurity is essential for individuals and organizations alike to ensure the confidentiality, integrity, and availability of their digital assets (NIST, 2018), (Idi Mohammed & Bade, 2019) .

Critical Information Systems	systems and assets, whether physical or virtual, are so vital to the SMME that the incapacity or destruction of such systems and assets would have a debilitating impact on the organization abilities to deliver on its goals and objectives, adapted from (NIST, 2018).
Cyber threat	refers to any malicious act or activity that seeks to exploit, damage, or gain unauthorized access to a computer system, network, or digital device. Cyber threats can take many forms, including viruses, malware, phishing attacks, hacking attempts, denial-of-service attacks, and other types of cybercrime. Cyber threats can come from a variety of sources, including individuals with malicious intent, criminal organizations seeking financial gain or other benefits, and nation-states engaged in espionage or other forms of cyber warfare. (NIST, 2018).
Risk Probability	is the likelihood or chance that a particular risky event will occur. It is a measure of the possibility that a risk will materialize and cause harm or damage to an organization or system. Risk probability is typically expressed as a percentage or a fraction, with higher values indicating a greater likelihood of the risk occurring (Institute, 2021).
Cyber risk Management	involves quantifying the probability and severity of risks, making it possible to support decisions about the most appropriate strategy to address them, such as inaction, avoidance, reduction, transfer, or insurance (Dupont, 2019).

1.9 Assumptions

The following were assumptions that were included in this study:

1. With increasing threat vectors, cyberattacks are inevitable.
2. Managers, heads of department, CEOs, CTOs, CIOs, would be open and free to discuss their cyber resilience implementation plans, their approach to cybersecurity plans, their actual cyber resilience performance, and identified vulnerabilities.
3. Cyber resilience is a critical requirement for SMMEs that use digital platforms.

1.10 Chapter Outline

The following section provides a brief overview of chapters in this research proposal report:

Chapter 1: Introduction

This chapter provides introduction to the research; it consists of the statement of purpose, and background of the study, which give context to the area of research and present the research problem. This is followed by research objectives, rationale, and delimitations of the study, Assumptions, and finally outline the chapter outline of the research study.

Chapter 2: Literature Review

This chapter reviews existing literature on cyber risk, cyber resilience, and cyber frameworks for addressing the problem statement and research objectives.

Chapter 3: Research Methodology

This section discusses the research methodology and how the study was conducted, as well as its findings and recommendations. It includes the research approach, design, and process was followed in collecting the research data. The chapter also includes the research instrument that was used, together with the sample taking into consideration the ethical issues and any study limitations that were applied.

Chapter 4: Presentation of Findings

This chapter details the quantitative findings of the collected data as well as raw data from survey research. The findings are presented in this chapter.

Chapter 5: Discussion of the Findings

This chapter discusses the findings of the collected sampling data from surveys and face-to-face interviews. It discusses findings in context with the research questions.

Chapter 6: Conclusions and Recommendations

This chapter to draws to conclusions the research questions and provide recommendations for research studies.

CHAPTER 2. LITERATURE REVIEW AND THEORETICAL FRAMEWORK

2.1 Introduction

SMMEs play a critical role in driving economic growth and job creation in many countries. Amid frequent cyber-attacks, coupled with limited resources and expertise in cybersecurity, cyber resilience has become a critical topic for individuals, organizations alike. This review explores the literature on cyber resilience and seeks to provide a critical analysis into existing literature on cyber resilience, focusing on key concepts, frameworks, challenges, and propose future direction into how SMMEs can enhance their cyber resilience and mitigate the risks of cyber incidents.

2.1.1 *Defining SMMEs*

SMMEs, in the context of Gauteng, South Africa, refer to Small, Medium, and Micro Enterprises. These enterprises are defined as distinct business entities managed by one or more individuals that must meet specific criteria outlined in the National Small Business Act of South Africa and as amended (Bvuma & Marnewick, 2020). The following is the criteria of classification of SMMEs in South Africa

Micro enterprises are enterprises with fewer than 10 employees, with an annual turnover of less than R10 million. While small enterprises are enterprises with greater than 10 employees but no more than 50 employees, with an annual turnover of between R10 million but no more than R50 million. Medium enterprises are enterprises with greater than 51 employees but no more than 200

employees, with an annual turnover of between R50 million but no more than R220 million.

However, in establishing whether the entity is small, micro, or medium of variation is the gross asset value of the enterprise, this is industry dependent. The act provides a detailed specification per industry.

2.1.2 *SMME contribution the economy*

SMMEs have been recognised as a crucial contributor to employment and economic growth in South Africa since 1994 (Agupusi, 2007). In recent years, there has been a renewed focus on the promotion of SMMEs due to the rising unemployment rate, the importance of SMMEs is further acknowledged in addressing inequality and poverty reduction, particularly among historically disadvantaged groups (Vuba, 2019). In an article by Business-Tech, SMMEs in South Africa are responsible for creating 4.8 million jobs, which is equivalent to 60% of the country's employment (Bhorat et al., 2018). Similarly, (Cheung, 2017) notes that SMMEs contribute approximately 42% to South Africa's gross domestic product (GDP) and account for about 60% of employment, representing over 90% of formal businesses. Accordingly, active SMMEs are not only crucial for driving productivity and growth (Rungani et al., 2018), but also are instrumental in reducing poverty and the unemployment rate (Bvuma & Marnewick, 2020) in the country.

2.2 Cyberspace Challenges among SMMEs

Despite the significant role they play, SMMEs are faced with numerous challenges such as, access to finance, markets, and skills development, as well as poor infrastructure, and inefficient bureaucracy. Since 2019, when the COVID-19 pandemic hit our shores in South Africa, many businesses have had to operate on various digital platforms to extend their market by reaching a greater number of customers (Gabriel *et al.*, 2021). This exposure to the digital world has brought

about further challenges to the already ailing business landscape, particularly for those who are unfamiliar with cybersecurity best practices. Studies conducted by (Carías *et al.*, 2020) show that SMMEs face several challenges when it comes to cybersecurity, including budget constraints, lack of employees with cybersecurity skills, management support, and commitment toward cybersecurity concerns in IT systems. These challenges make it difficult for SMMEs to implement effective cybersecurity measures and to protect their critical information systems from potential cyber threats thereby, leaving SMMEs systems vulnerable to cyber-attacks due to inadequate cybersecurity protection.

Cybercriminals exploit various vulnerabilities in computer systems, networks, and software to gain unauthorized access to sensitive information or cause damage to the system. Some of the most common vulnerabilities that cybercriminals exploit includes, weak passwords, unpatched software, outdated operating systems, social engineering tactics such as phishing emails or phone calls, and unsecured Wi-Fi networks. Cybercriminals may also use malware such as viruses, worms, and Trojan horses to gain access to a system or steal data. Additionally, they may exploit human errors such as employees clicking on malicious links or downloading infected files (NIST, 2018), (Cahyono *et al.*, 2022). This means that cybercriminals can exploit any weakness in a computer system, employee, or network that allows them to gain unauthorized access or cause harm. These vulnerabilities coupled with lack capacity weaken the position of SMMEs to effectively anticipate, withstand, recover from, and adapt to every potential cyber threat that may negatively affect them. Accordingly, lack of management support and perceptions of leadership among SMMEs who perceive their firm to be less technologically complex or smaller in size compared to larger corporations, are at an even greater risk to suffer from to cyber-attacks (Salah Kabanda *et al.*, 2018,); (Chatterjee, 2020). Cybercriminals can exploit any vulnerabilities in any computer information system in cyberspace regardless of size, or form. Therefore, SMMEs are not immune to cyber-attacks which expose them to cyber related risk.

Considering the limited capacity and vital role of SMMEs in the economy and increasing cyber threat vectors, traditional cybersecurity approaches that focus

on known threats are insufficient in protecting SMMEs from cyberattacks.. Studies by (Chatterjee, 2020) show that embedding cyber resilience capabilities can help SMMEs to manage cyber-related risk. Therefore, by addressing internal barriers that hinder the implementation of cybersecurity measures is essential to enhancing cybersecurity practices within SMMEs. The adoption of a cyber resilience approach, frameworks is becoming increasingly important for SMMEs, (Solms *el al* 2014), (Carías *et al.*, 2020). Fundamental to building cyber resilience capability depends on the SMME's ability to identify which critical information systems are crucial for the achievement of the organisation mission objectives (NIST, 2018). This ensures that, in the event of cyberattacks, the SMMEs are able to secure assets that are critical to the business objectives to remain protected and business continuities to operate with minimum downtime, thus ensuring cyber resilience of SMMEs.

2.3 Addressing cybersecurity challenges can be a daunting task for SMMEs, but it is essential for their survival and growth in the digital economy. By recognizing the unique challenges they face, SMMEs can take steps to mitigate risks, such as prioritizing cybersecurity investments, seeking external expertise, and adopting a proactive security posture, (Salah Kabanda *et al.*, 2018,); (Chatterjee, 2020) Gabriel *et al.*, (2021). Collaborative efforts, such as industry partnerships and government initiatives, can also play a crucial role in supporting SMMEs in their cybersecurity journey. Therefore, by enhancing their cybersecurity resilience, SMMEs can protect their critical infrastructure systems, maintain customer trust, and ensure long-term business success.Cyber Resilience

Since the 2012 World Economic Forum meeting in Davos, there has been a growing attention and usage of the term cyber resilience for individuals, businesses, and societies. While the study of cyber resilience is relatively a new

field, and researchers are still developing the terminology and its frameworks, the term draws its meaning from various disciplines including, ecological, social, psychological, organizational, and engineering domains. For instance, in engineering, resilience entails the ability of systems to anticipate and adapt to the potential for surprise and failure, signalling a shift in safety paradigms that recognize the importance of system coping in situations where prevention is not feasible (Zwass, 2010). Ecological resilience, in contrast, focuses on a system's capacity to absorb and endure shocks, with an emphasis on persistence (Holling, 1996). However, based on these interpretations, resilience is progressively understood as a dynamic process with the ability to foresee, assimilate, recover from, and adjust to unfavourable circumstances. This definition has been embraced by various global organizations and governance bodies, including those operating in cybersecurity (Connolly et al., 2017; Larkin et al., 2015). Cyber resilience is the ability to continuously deliver the intended outcome despite adverse cyber events (Björck *et al.*, 2015). It is defined as the capacity to withstand, recover from, adapt to, and evolve from cyber incidents, thereby minimize cyber risk (Dupont, 2019). Similarly, (Chatterjee, 2020) defines cyber resilience as a comprehensive approach that encompasses both technical and non-technical aspects of cybersecurity, which extends from cybersecurity, which requires SMMEs to develop measures and strategies to prevent and protect against cyber-attacks. Accordingly, this study adopts Björck et al. (2015); (Omera Khan, 2015) to describe cyber resilience as the capacity of a system to recover from the consequences of a cyber-attack and continuously deliver the intended outcome despite adverse cyber events.

While cybersecurity focuses on preventing cyber threats and attacks from compromising the confidentiality, integrity, and availability of information assets. Cyber resilience focuses on assuring that only critical assets are protected. It goes beyond just protecting IT systems and focuses on the organization’s ability to anticipate, detect, withstand, recover from, and evolve after cyber incidents (Carías *et al.*, 2020) to ensure business continuity and operational functionality despite any type of adverse situation (Björck *et al.*, 2015)

The terms cyber resilience and cybersecurity have often been confused to mean the same thing and yet have very distinctive characteristics. **Table 1** below provides a summary of their distinctive characteristics.

Table 1: Characteristics of Cybersecurity vs. Cyber resilience

Aspect	Cybersecurity	Cyber Resilience
Objective	Protect IT systems	Ensure business delivery
Intention	Fail-safe	Safe-to-fail
Approach	Apply security from the outside	Build security from within
Architecture	Single layered protection	Multi layered protection
Scope	Atomistic, one organization	Holistic, network of organizations

Source: Björck, Henkel, Stirna, & Zdravkovic, (2015)

From these characteristics, it is evident that cyber resilience extends beyond the traditional objective of cybersecurity, focusing on the overarching goal of ensuring business delivery even in the face of adverse cyber events Björck *et al., (*2015). The essence of a resilient system lies in its ability to function in a fail-safe manner while also being capable of controlled failure, denoted as "safe-to-fail." The cyber resilience approach surpasses conventional surface-level security measures by necessitating integration into the intrinsic workings of IT systems and overarching business operations. This involves embedding resilience as an integral element rather than an additional feature. The architecture of a resilient system is characterized by its capacity for partial failure, featuring multiple layers of protection designed for recovery, in contrast to a rigid outer shell. The scope of a cyber-resilient analysis expands beyond individual systems or organizations to encompass a broader network of interconnections and systems, acknowledging the collective vulnerabilities and strengths that contribute to overall resilience. This comprehensive perspective serves as the foundation for a thorough vulnerability analysis and a wellspring of resilience.

2.4 Importance of Cyber resilience

There are several compelling reasons why policymakers, researchers, and the general population advocate for the necessity of promoting cyber resilience. The

primary reason is that society is increasingly being reliant upon complex and interconnected cyber systems to conduct daily activities (Linkov & Kott, 2019) . These activities may range from managing personal finance to managing defence capabilities or controlling a vast web of aircraft traffic. Although reliance on internet capabilities have brought about immense increases in efficiency of service delivery, it has also been subject to a diverse body of threats from nefarious hackers, groups, and even state government bodies, Linkov & Kott, (2019). Attack targets have become diverse with impact felt beyond financial losses, encompassing security, social disorder, and potential ramifications in warfare (Kott et al., 2015). To mitigate these challenges, several frameworks have been proposed and applied (Carais *et al.*, 2021; (Mbanaso *et al.*, 2019a). The following paragraph discusses these in detail.

2.5 Cyber Resilience Frameworks

In the ever-growing landscape of cyber threats, organizations of all sizes are seeking robust frameworks to assess and improve their cyber resilience (Crane, 2021; Madondo, 2021) (Williams & Manheke, 2010) A number of cyber resilience frameworks have developed, some of which have been found to lack in design that is applicable to SMMEs. However, three prominent models have emerged, including CERT Resilience Management Model (CERT-RMM) (Matt Trevors & Wallen, 2017), the CR-SAT (Carias, 2021), and Cyber Resilience Maturity Model (CRMM) (Mbanaso *et al.*, 2019b). Although their approach may differ to some extent, they are all linked to the NIST framework to derive to adoption of conceptual framework.

Resilience Management Model (CERT-RMM)

The CERT Resilience Management Model (CERT-RMM) is a comprehensive framework that was developed through a comprehensive review of 800 existing codes of practice in security, business continuity and IT operations, see (Caralli *et al.*, 2010). The model outlines 26 processes that aim at fostering the capabilities necessary for operational resilience to become a repeatable, predictable, manageable, and improvable process under an organization’s active and direct control. The CERT-RMM was developed in close collaboration with the

Financial Services Technology Consortium with the aim of creating a reference model for measuring and managing operational resilience Caralli *et al.,* (2010).

Since inception, researchers have applied CERT-RMM in various settings. For example, a study that aimed at exploring the practical and successful applications of the CERT-RMM (Mehravar, 2013), contends that the CERT-RMM is the most modern and comprehensive framework for managing operational resilience in variety of organisations. In another study conducted a comparative analysis of the (Sharkov, 2020) conducted a comparative analysis to ascertain the applicability and usefulness of the CERT-RMM in relation to Cybersecurity Capacity Maturity Model for Nations, C2M2 (Cybersecurity Capability Maturity Model to develop cybersecurity strategies at a sectoral and national level. The findings reveal that to assess the cybersecurity and cyber resilience of a sector, community, country, or region, a unified approach to define goals and measurement indicators is needed. Among the comparisons, it was noted that the Capability maturity models provide such a mechanism since they implement a similar architecture and regardless of possible differences in scope and definitions of domains.

These studies demonstrate the practical application of CERT-RMM in developing targeted improvement roadmaps for organizations. By following these roadmaps, organizations can focus their efforts on the areas that will have the greatest impact on their resilience goals. However, existing literature primarily presents capability maturity models, designed to delineate processes already in practice and evaluate their integration into a company's culture (Caralli *et al.*, 2012). Consequently, this tool may require prior experience and an established operationalization of cyber resilience within organizations to be effectively utilized. Furthermore, There is limited research that demonstrates how to apply the CERT-RMM to organisations in a developing economy like South Africa, especially on critical information systems of SMMEs in Gauteng

Cyber Resilience Self-Assessment Tool (CR-SAT)

The CR-SAT tool was developed by Carias, *et al.* (2021) to help SMMEs improve cyber resilience through a systematic continuous process improvement. It

provides specific essential guidance for cyber resilience practices that can help decrease the impact of cybersecurity risk. It recommends a framework with 11 essential domains and 33 practical polices such as a domain could be asset management and associated practical policy this could be making a list of asset inventory and identifying the SMME critical assets. These recommended essential domains with associated practical practices have their foundation in the NIST framework Carias, *et al.* (2020).

The CR-SAT framework is designed to be user-friendly and adaptable, making it well-suited for SMMEs with limited resources and expertise. The framework provides a structured approach that is easier to implement and understand compared to more complex frameworks like CERT-RMM or CRMM. It is specifically developed for SMMEs, considering their unique challenges and requirements. It offers a practical and focused approach to assessing cyber resilience, making it more relevant and applicable for SMMEs Carias, *et al.* (2020).

CR-SAT emphasizes self-assessment, enabling the SMME to evaluate their cyber resilience capabilities independently. This self-assessment empowers the SMME to identify area of improvement and take proactive measures to enhance their cyber resilience Carias, *et al.* (2021).

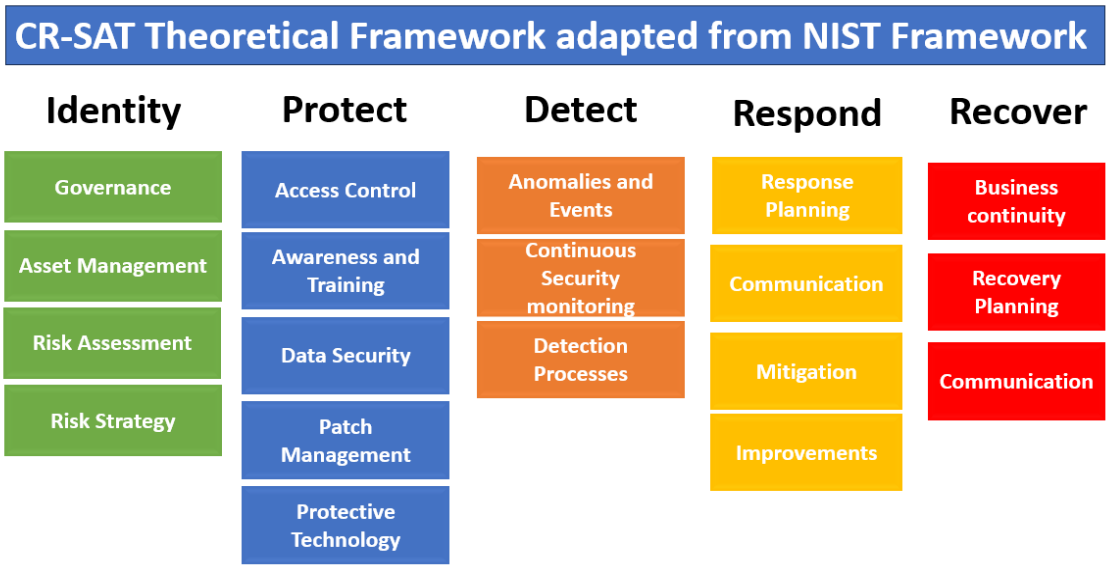
However, the CR-SAT framework is not without limitations while the CRMM and CERT-RMM offers a more comprehensive, scalable, and detailed approach to assessing cyber resilience, which may be more suitable for organizations requiring a thorough evaluation, CR-SAT may not be able to provide a more in-depth assessment (Carpenter *et al.*, 2014).

Where there is budget constraints Carias, *et al.* (2021).CR-SAT recommends prioritizing essential cybersecurity measures and risk mitigation strategies. This approach therefore makes it feasible for model to be adapted to specific situations in the context of the SMME.

Against this backdrop it can be noted that cyber resilience is influenced by various critical success factors, including employee awareness and training, patch management, incident response and business continuity, risk assessment and

management, access control and privilege management. This study adopted the CRT-SAT theoretical framework, adapted from NIST framework as depicted in figure 1 below, This will be use to explore critical success factors for SMMEs in Gauteng to understand their approach to cyber resilience, to explore the extent to which practices and procedures are exhibited in the SMME.

Figure 1: Theoretical Framework adapted from NIST Framework



Adapted from NIST Framework (NIST, 2014)

2.6 Assessing critical success factor practices implemented

CR-SAT framework provides the progression model, scale rating moderated descriptors to self-assess how well the SMME have implemented the guide or practices in each domain or policy. By choosing the description that best fits their current situation, the descriptors can be mapped to a cyber resilience rating scale where 0 demonstrates that the organisation is not doing much in terms of practical implementation of policy of a particular domain, and 5 would mean the organisation demonstrate high levels of cyber resilience maturity, in a sense that the practices have been embedded in the organisation and the organisation can

deal with increasing cyber threat landscape Carias, *et al.* (2021. For example, in Table 2 below

Table 2: Measuring cyber resilience, scale rating and moderated descriptors Carias, *et a*l. (2021).

Domain and Policy	**Scale rating and moderated descriptor**	
	Rating	**Moderated Descriptor**
Domain: Governance **Policy:** G2 Comply with cyber resilience regulation	0	No awareness or effort
	1	The company has identified the cyber resilience or cybersecurity related laws and regulations that directly concern their activity
	2	The company does its best to comply with the most directly related cyber resilience, cybersecurity laws and regulations
	3	The company tries its best to comply with regulations that have been identified by the internally auditing team which are being complied with and which are still in progress
	4	Company starts exploring law and regulation that can directly concern their and sees added value in complying with these laws to improve their cyber resilience
	5	The company continually complies with more demanding regulations driven by their own cyber resilience implementation and not simply with the intention of complying

2.7 Cyber Resilience Critical Success factors

SMMEs face unique challenges in general when it comes to ensuring the cyber resilience of their critical information systems. This literature review aims to explore the critical success factors and best practices that can help SMMEs in Gauteng enhance their cyber resilience.

Various literature material was reviewed to identify baseline essential practices areas that are key to achieve cyber resilience of critical information systems. This included The South African Reserve Bank Prudential Authority and the Financial Sector Conduct Authority (Authority, 2022). The Carnegie Mellon University Software Engineering Institute (Matt Trevors & Wallen, 2017) which proposes the CERT Resilience Management Model (CERT-RMM) which comprises of 11 baseline practice areas. Various academic research papers, and CR-SAT conceptual framework which proposes the SME cyber resilience framework.

Various studies reveal baseline practice factors that are key for SMMEs to achieve cyber resilience of their critical information systems. These include studies by (Kott & Linkov, 2021), (Groenendaal & Helsloot, 2021), Carias,) (2020), (Solms, 2019), (Chatterjee, 2020).

Therefore, some of these baseline critical success factors were further reviewed to help answer the objectives and research questions of this study.

2.7.1 *Cybersecurity Awareness and Training*

Carias, (2020), Walaza et al., (2020), (Cilliers & Chinyamurindi, 2020), (Kelly *et al.*, 2022) highlights that employee awareness and training in enhancing cyber resilience for SMMEs. The study emphasizes the need for conducting the SMMEs cyber skills analysis, educating employees about cyber threats, safe online practices, and the importance of reporting incidents. Regular training sessions can help create a security-conscious culture within the organization.

2.7.2 *Risk Assessment and Management*

Several studies (Dupont, 2019), (Radanliev *et al.*, 2019), (Chatterjee, 2020), (Marsh, 2021), (Loonam *et al.*, 2022), (Malatji *et al.*, 2020), highlight that risk

assessment and management as crucial factor in cyber resilience. These studies recommend conducting a comprehensive risk assessment to identify potential vulnerabilities and threats. SMMEs should assess their information systems, data assets, and business processes to understand their risk landscape. This assessment should be followed by the development and implementation of a risk management strategy that includes preventive, detective, and corrective measures.

2.7.3 *Incident response and business continuity*

The NIST, (2022) provides a comprehensive guidance on developing and implementing effective incident response and business continuity plans. NIST recommends that having a well-defined incident response plan is crucial for SMMEs to minimize the impact of cyber-attacks. The plan should outline the steps to be taken in the event of a security breach, including incident detection, containment, eradication, and recovery. Additionally, SMMEs should develop business continuity plans to ensure the continuity of critical operations during and after a cyber incident.

Studies by Carias, (2020) highlights business continuity planning as focussing on ensuring the continued operation of critical business functions in the face of disruptions, including cyber incidents. It involves identifying potential risks and developing strategies to mitigate them, such as backup and recovery procedures, redundant systems, and alternative work arrangements. Business continuity plans aim to minimize downtime, protect critical assets, and enable the organization to recover and resume normal operations as quickly as possible.

2.7.4 *Access Control and Privilege Management*

The NIST framework provides definition of access control to include authenticating, verifying the identity of users, authorizing determining what resources they can access, and accounting and tracking user activities for auditing purposes. Access control can be implemented through various methods such as passwords, biometrics, access control lists, and role-based access control.

Privilege management focuses on granting and managing user privileges or permissions within a network infrastructure. It involves assigning appropriate levels of access rights to users based on their roles and responsibilities. Privilege management helps prevent unauthorized access and limits the potential damage that can be caused by compromised accounts. It includes practices such as least privilege, where users are granted only the minimum privileges necessary to perform their tasks, and regular review and revocation of privileges for users who no longer require them.

2.7.5 *Network and Perimeter Security*

(Carias, 2020) highlights the need for SMMEs to implement robust network security measures to Secure their network infrastructure: SMMEs should implement practices, such as using firewalls, intrusion detection systems, and secure Wi-Fi networks. Regular network monitoring and patch management are also essential to identify and address vulnerabilities promptly.

2.7.6 *Patch Management*

Carias, (2020) Recommends that SMMEs should have a mechanism to detect and monitor network and software patches. Subscribe to vendor alerts, security mailing lists, or automated patch management programs.

Before implementing patches, SMMEs should assess their effect on network infrastructure and verify compatibility and stability. This reduces patch-related issues. SMMEs should deliver fixes quickly after testing. Depending on network size and complexity, automated patch management solutions or manual installation may achieve this. After patch distribution, SMMEs should monitor SMMEs should create a patch deployment policy including methods, responsibilities, time to carry out updates. This policy should be evaluated and modified to reflect changing threats and software changes.

2.7.7 *Data Backup and Recovery*

Salah Kabanda, (2018,) highlights good practices for data backup and recovery. These include regular back up of data, use of multiple backup test backups, store backups securely, implement encryption, document backup procedures, train employees on the importance of data backup governance.

Following these steps can enhance SMMEs data backup and recovery capabilities, reducing the risk of data loss and minimizing downtime in the event of a data breach or system failure.

2.7.8 *Vendor and Third-Party Management*

Björck et al., (2015) highlights the SMMEs need to ensure that their vendors and third-party partners are also resilient to cyber threats and have appropriate security measures in place to protect their shared systems and data. This can be achieved through effective risk management practices, such as due diligence, regular assessments, and contractual agreements that outline security requirements and responsibilities.

This involves evaluating factors such as the sensitivity of the data or systems being shared, the criticality of the services provided, the vendor's security practices, and their record of accomplishment in managing security incidents.

Literature reveals that vendor management include practical steps like reviewing their security policies and processes, conducting security audits or assessments, and requesting documentation on their security controls and practices.

2.7.9 *Continuous Monitoring and Threat Intelligence*

(Carias, 2020) highlights implementing continuous monitoring tools and threat intelligence systems can help SMMEs detect and respond to cyber threats in real-time. These tools can provide insights into emerging threats and vulnerabilities, enabling proactive security measures.

This can be done by deploying various controls and sensors, such as intrusion detection systems, network intrusion detection systems, security information and event management systems, and log monitoring tools. Real-time Monitoring of network traffic, system logs, user activities, and other relevant data sources. This allows SMMEs to detect and respond to security incidents promptly. Incident detection and response, vulnerability management (Carias *et al.*, 2021).

The research by (Carias *et al.*, 2021) found that SMMES achieved cyber resilience in the information security process domain by focusing on the mitigation of risks, threats, and vulnerabilities. This had a positive impact on information security, business continuity management process domains.

2.3.10 Cyber resilience critical success factors conclusion

These critical success factors discussed in point 2.7.1 to 2.7.9 can help contribute to the cyber resilience of SMMEs in Gauteng, enabling them to effectively protect their digital assets and mitigate the impact of cyber threats. By prioritizing these factors, SMMEs can enhance their ability to withstand and recover from cyber incidents. Understanding the extent to which these critical success factors are implemented, can help establish cyber resilience measure.

2.8 Measuring critical success factors to cyber resilience.

Drawing from literature reviewed it can be concluded that measuring cyber resilience by critical success factors involves assessing the SMMEs critical Information systems and its ability to resist, recover, and adapt from cyber incidents and compromises. This was achieved by interrogating the critical information systems using the critical success factors identified in literature and by answering the research questions.

CHAPTER 3. RESEARCH METHODOLOGY

3.1 Introduction

In the previous chapter a literature review on cyber resilience and related frameworks that can assist in mitigating the cyberspace challenges SMMEs face has been discussed. This chapter focuses on the research methodology used in the study. The chapter begins with a discussion on the research design and research approach. Thereafter, an outline of the sampling strategy is presented. This includes a discussion of the population, sampling frame, sampling methods and the sample size. Data collection methods, as well as procedures for data analysis, also form part of the discussion.

According to (Walther *et al.*, 2013) (Walther *et al.*, 2013)research seeks to find answers to a specific question by the process of planning, executing, and investigating. A systematic approach is however required to get reliable answers to the research problem as well as aiming at producing a credible report that others can understand and believe Walther *et al.*, (2013).planning, executing, and investigating with the sole purpose of trying to find answers to a specific question (Walther *et al.*, 2013). Accordingly, this chapter aims at discussing the methodological approaches used in the study

3.2 Philosophical Underpinnings and Research Paradigms

Exploring the nature of reality and the generation of knowledge has been a topic of prolonged debate in the realm of research. Since its inception, research philosophy or paradigms have provided guidance to researchers in their study endeavours (Cohen *et al.*, 2017) According to (Mertens, 2006) research is defined as a systematic inquiry involving the collection, analysis, and interpretation of data to create knowledge or to describe, predict, and control philosophical phenomena. While research heavily relies on the researcher's subjective assumptions,(Aliyu *et al.*, 2015) argue that research paradigms offer a framework for building theories and shaping one's understanding of the interconnectedness of things. Hence, a comprehensive comprehension of these

research paradigms is facilitated when viewed through the lenses of ontological and epistemological assumptions, which, in turn, dictate the methodology (Durrheim, 1996) This, in effect, influences the selection of research questions, the nature of research instruments, research designs, data collection methods, sampling procedures, and approaches to data analysis(Madondo, 2021)

Ontological assumptions pertain to our comprehension of the actual world or the true nature of things (Collinson *et al.*, 2011),In contrast, epistemology refers to the branch of philosophy examining how individuals acquire and justify knowledge (Saunders *et al.*, 2019). However, as noted by (Scotland, 2012) the philosophical assumptions of ontology and epistemology are essentially "conjecture," meaning that research paradigms stemming from these assumptions cannot be empirically proven or disproven. This uncertainty has led to what some describe as "research paradigm wars" (Denzin, 2010; Symonds & Gorard, 2010). Consequently, researchers often grapple with the challenge of aligning methodologies and methods with the theoretical foundations of their research (Crotty, 1998). Nevertheless, the primary paradigms contending as the preferred frameworks to inform and guide inquiry include positivism, post-positivism, constructionism, and critical theory (Guba *et al.*, 2005).

The positivist research paradigm employs scientific research methods like statistical analysis and the generalization of findings, operating on the assumption that research aims to prove or disprove a hypothesis (Schulze *et al.*, 2014). Post-positivism represents the conventional form of research, particularly in quantitative research, emphasizing causal relationships as used in experimentation and correlational studies Scotland, (2012). The constructivist approach posits that the world is constructed, interpreted, and experienced by individuals in their interactions with each other and broader social systems (Guba & Lincoln, 1985:110). Despite the potential for individual views to be incomplete or subject to alteration based on associations, the constructivist paradigm maintains that the researcher is an active participant in the research process Schulze *et al.*, (2014). Table 3 provides a summary of scientific paradigms and their classifications.

Table 3: Categories of Scientific paradigms and their classifications

Classification	Research paradigm			
	Positivism	**Critical theory**	**Constructivism**	**Realism**
Ontology	Reality is real and apprehensible	"Virtual" reality is shaped by social, economic, ethnic, political, cultural, and gender values, crystallises over time	Multiple local and specific "constructed" realities	Reality is "real" but only imperfectly and probabilistically apprehensible
Epistemology	*Objectivist:* findings true	*Subjectivist:* value mediated findings	*Subjectivist:* created findings	*Modified objectivist:* findings probably true
Common methodologies	*Experiments/ surveys:* verification of hypotheses: chiefly quantitative methods	*Dialogic/dialectical:* researcher is a "transformative intellectual" who changes the social world within which participants live	*Hermeneutical / dialectical:* researcher is a "passionate participant" within the world being investigated	*Case studies/convergent interviewing:* triangulation, interpretation of research issues by qualitative and by some quantitative methods such as structural equation modelling
Note: Essentially, ontology is "reality", epistemology is the relationship between that reality and the researcher, and methodology is the technique used by the researcher to investigate that reality.				

While noting that research paradigms guide research, (Creswell *et al.*, 2003) advise that researchers should focus on adopting a technique that works and provides solutions to the research problem at hand. For that reason, this study was guided by the constructionism research paradigm to qualitatively explore cyber resilience (CR) of small, medium, and micro enterprises (SMMEs) in Gauteng.

3.3 Research Design

A research design is defined as "a master plan that outlines the methods and procedures for collecting and analysing the necessary information." Essentially, the purpose of a research design is to ensure that the evidence gathered in a

research project allows the researcher to answer the initial question as clearly as possible (Tierney, 2002) Consequently, the selection of a research design hinges on whether the research is exploratory or conclusive (Malhotra, 2010). An exploratory research design is appropriate for a problem that lacks a clear definition. Conversely, conclusive research is crafted to assist the researcher in evaluating and selecting a better course of action in each situation. Moreover, a conclusive research design can be either descriptive or causal. Descriptive research is conducted when there is a need to thoroughly explain or depict data from the population under study (Mitchell *et al.*, 2010)It can be utilized to test a hypothesis about any variable in any situation, investigating questions of who, where, and when, describing how one variable relates to another Mitchell *et al.*, (2010). In this scenario, the research question is planned or structured, and the collected information can be statistically generalized to a population (Malhotra, 2010:106). To address the research questions posed in this study, an exploratory research design was employed.

3.4 Research Approach

A research approach encompasses the overall plans and procedures, of both the broad steps and detailed methods of collecting, analysing, and interpreting research findings (Crotty, 1998). Researchers can choose from three research approaches: qualitative, quantitative, and a mixed-method approach (Creswell, 2013). Qualitative research methods, as noted by (Trim & Lee, 2004), are employed to comprehend complex issues, where researchers gain insights through a focused examination of case studies and grounded theory. Qualitative research typically involves small samples, and its results are not generally applicable to a larger population. On the other hand, quantitative research methods emphasize statistical or numerical analysis of data collected through questionnaires or surveys to test theories and explore relationships among variables approach (Creswell, 2013). Quantitative research aims to quantify research data to obtain conclusive evidence that can be extrapolated to a broader population (Malhotra, 2013). In quantitative research, closed-ended, narrow questions are employed to gather measurable and observable data for testing variables using instruments like questionnaires Creswell, (2013). Considering

these characteristics, a qualitative research approach was employed to explore this cyber resilience (CR) of small, medium, and micro enterprises (SMMEs) in Gauteng.

3.5 Sampling: Design and Procedures

Sampling is a structured process with five steps that assist the researcher in delineating the target population, establishing the sample frame, choosing a sampling method, ascertaining the sample size, and carrying out the sampling procedure (Malhotra *et al.*, 2007). An intricately devised sampling design significantly influences the data quality and research outcomes (Malhotra & M, 2012). The subsequent sections provide a more elaborate explanation of each step.

3.5.1 *Target Population*

(Burns *et al.*, 2005) describes a population for research to include all the elements such as, individuals, objects or substances that meet a certain criterion for inclusion in a given universe. A target population, therefore, reflects a collection of elements or objects that possess the information the researcher is seeking and for who inferences could be made (Malhotra & Peterson 2014). Accordingly, the target population for this study comprised all SMMEs in Gauteng.

3.5.2 *Sampling Frame*

A sampling frame, also described as a representation of the elements of the target population (Cant, 2003), allows the researcher to identify a list or sets of units in the population that best describes the target population. The sampling frame for this study comprised a selection of SMMEs operating in Gauteng.

3.5.3 *Sampling techniques*

Sampling techniques are methods that dictate how the sample was selected (Cant, 2003). While it is important that the researcher chooses an appropriate technique to draw a sample, the researcher can choose between probability and non-probability sampling techniques (Ghauri & Grønhaug, 2005), In probability sampling, each unit has a known chance of being selected to be part of the

sample and the results drawn from such a sample can be generalised to the population at large. Examples of probability sampling include simple random sampling, systematic sampling, stratified sampling, and cluster sampling Cant, (2003). Non-probability sampling relies on the researcher's personal judgement. Whereby the chance that elements in the population would be included in the sample is not known. Examples of non-probability sampling techniques include convenience sampling, judgemental sampling, quota sampling and snowball sampling Cant, (2003). Going into a detailed explanation of the different characteristics, advantages, and disadvantages of these types of sampling techniques is beyond the scope of this study.

However, after careful consideration and according to the researcher's personal judgement, purposive sampling technique was employed in the study. Purposive sampling denotes a non-probability sampling technique where researchers select participants based on specific characteristics or criteria relevant to the research study. This method allows researchers to target individuals who possess the information or experiences necessary to address the research questions effectively.

3.5.4 *Sample Size*

According to Malhotra and Birks (2007), a sample size indicates the number of elements to be included in the study. While the process of sample size determination can be daunting and challenging for the researcher, Cant, (2003) advises that the sample size must be large enough to ensure that reliable and valid conclusions could be made about the population. However, the process can be complex due to several qualitative and quantitative factors that must be considered first (Malhotra *et al.*, 2007). This study employed the qualitative approach to determine the sample size.

Determining the sample size for a qualitative study is a complex and context-specific process. While there is no one-size-fits-all answer, several factors should be considered. According to (Johnson *et al.*, 2020) the characteristics of the study, such as the research objectives, the nature of the phenomenon under investigation, and the quality of data, should guide the sample size determination.

Saturation, which occurs when adding more participants does not result in obtaining additional information, is a key goal in qualitative research. As a general recommendation, in-depth interviews often aim for sample sizes between 20-30 to achieve this saturation. The type of qualitative study and the research methods used also influence the appropriate sample size. Ultimately, the focus in qualitative research is on the quality of data obtained rather than the quantity of participants, and the sample size should be determined to achieve the research objectives and data saturation. The sample size for this qualitative study comprised SMMEs owners in Gauteng (N=15).

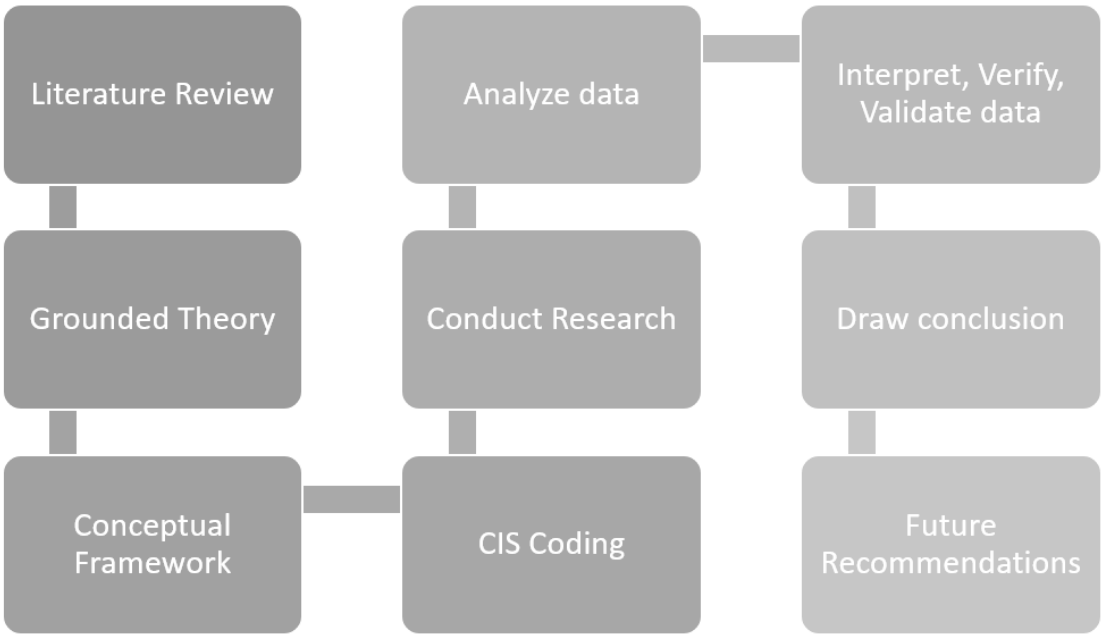
3.5.5 *Critical Success Factors and Best Practices*:

This study is based on the understanding that cyber resilience is influenced by various critical success factors, including employee awareness and training, patch management, incident response and business continuity, risk assessment and management, access control and privilege management.

3.5.6 *Develop Research Framework:*

The research framework followed to examine critical factors that influence cyber resilience was as per Figure 2 below.

Figure 2: Research Framework



3.6 Data Collection

Data collection involves a precise and systematic gathering of opinions and views for the purposes of answering a research problem (Murthy & Bhojanna, 2010). There are two main types of sources for data namely, primary, and secondary data sources: While secondary data sources are those that are readily available and were previously collected for other purposes, for example data previously collected by international organisations or the government, primary data are data that are collected for a particular research problem (Ghauri & Gronhaug, 2010). This study used secondary data sources to conduct an extensive literature study. Furthermore, the study employed primary data collection process to explore cyber resilience (CR) of SMMEs in Gauteng.

3.6.1 Interview Guide

Developing an interview guide for qualitative research followed several steps. First, the research objectives and the population of interest were carefully considered. Then, open-ended questions are crafted to explore and understand

the richness and complexity of human experiences, opinions, and narratives on cyber security, cyber resilience, and related experience. These questions aimed to reveal subjective truths which was used to identify initial themes or areas that were explored further in interviews. Throughout the development process, it was important to ensure that the focus did not deviate from the research objectives and that the questions were appropriate and well-aligned with the research goals. The design of the questionnaire was tailored to suit the medium of the survey, whether it is conducted face to face, by phone, or online. Finally, it was essential to review the questionnaire based on the output information that was collected from the first interview, as this information was not addressing the research questions. The research questions for this study were developed based on the CR-SAT framework for SMMEs.

3.6.2 *Data Collection:*

Data collection is a fundamental component of the research process, encompassing a methodical and systematic collection of opinions and perspectives to address a research problem (Murthy & Bhojanna, 2010:241). This may involve various methods such as, interviews, and analysis of organizational documents and incident reports. Furthermore, audiovisual digital materials may be collected to draw more insights. This study conducted semi structured interviews to collect data. Data collection took place between the period of November 2023 to December 2023 after the ethics approval was obtained. Ten interviews were scheduled and took place, nine interviews took place on Microsoft teams, one took place in person at a venue convenient to the SMME that was being interviewed. Two of the meetings that took place no data was collected as the CEO were not well informed with cyber resilience nor cyber security, they promised to set up a meeting with a person within their organization who was better informed with cyber security and cyber resilience, and this never materialised. The open-ended semi structured interviews took an average of thirty (30) minutes per interview. All these meetings were recorded and transcribed. Saturation was reached when SMME No7 was interviewed as analysed data of output of emerging themes from new data collected did not draw

new insights. A decision was made to stop recruiting for potential SMMEs to be interviewed at SMME No8.

3.6.3 *Data Analysis:*

Data analysis involves converting unprocessed data into valuable information that facilitates drawing conclusions about a phenomenon (Ghauri & Grønhaug, 2005). Effective data analysis necessitates the researcher to establish analysis goals by determining the information required to fulfil the research objectives Cant, (2003).

Collected data was analysed thematically, data was transcribed, coded, and categorized into themes and sub-themes. The analysis of data was guided by the research objectives, NIST CR-SAT adapted framework and scale rating and moderated descriptors.. The trustworthiness of the analysis was ensured through prolonged engagement with transcribed data, and member checking to ensure transcribed represented the approach to cybersecurity practices of the SMME. Emerging themes and patterns out of data collected of the SMME were mapped to the NIST CR – SAT adapted theoretical framework, cyber resilience approach was summarised using scale rating and moderated descriptors, The findings of main process domains content analysis are represented in a table format. These findings were further reviewed to interpret findings and to understand how SMMEs in Gauteng approach cybersecurity, to understand which key dimensions factors that influence cyber resilience were employed by the SMMEs. The outcomes of the analysis were used to recommend areas of focus, investment, and prioritization to enhance cyber resilience of SMMEs in Gauteng.

3.7 Possible Limitations and Challenges of the Study

As highlighted in Kott & Linkov (2021) and (Linkov & Kott, 2019), measuring cyber resilience is a complex task. There is a lack of rigorous and qualitative methods to measure cyber resilience implementations outcomes. The meaning of cyber resilience, the term itself is often misunderstood. Traditional risk assessment

approaches may not adequately account for the interdependencies and cascading effects in complex and interconnected systems.

Using a scale rating system with moderated descriptors to measure outcome as classified in CR-SAT framework present limitations due to subjective nature of such rating systems, this can introduce variability in the interpretation of findings.

The rapidly evolving threat landscape poses challenge for cyber resilience assessments, (Carias et al., 2020). This means that cyber resilience measure may only be valid at the time of measure.

The use of purposive sampling, meant that potential interviewed candidates were recruited through non-probability sampling where SMMEs selected had similar characters, recruiting candidates proved to be a challenge. Therefore, interviewed candidates may not be truly a representative of SMMEs in Gauteng s to draw concrete cyber resilience measure of SMMEs in Gauteng.

3.8 Quality Assurance

To ensure the quality of the research, the study adhered to the criteria for trustworthiness in qualitative research proposed by (Morse, 2015). This study used strategies such as, developing clear research objectives, interviewing CEO, CTOs, CIOs, heads of department who had good understanding on the SMMEs cybersecurity approach. Conducting cyber resilience assessments involve accessing sensitive information and data, raising concerns about privacy and confidentiality. Ensuring the protection of participants' data and complying with ethical guidelines is essential to address these quality assurance concerns.

3.8.1 *External Validity or Transferability*

A study by Morse (2015) provides insights into strategies for ensuring external validity or transferability, it recommends several strategies to achieve rigor in qualitative research, which are essential for enhancing external validity. These strategies include prolonged engagement, persistent observation, and thick, rich description; inter-rater reliability, negative case analysis; peer review or debriefing; clarifying researcher bias; member checking; external audits; and

triangulation. Incorporating these strategies helped address external validity and transferability issues.

3.8.2 *Internal Validity OR Credibility*

By reflecting on the researcher's own biases, assumptions, and perspectives throughout the research process, as referenced (Bryant, 2007). Reflexivity helps to ensure that the researcher's influence on the research is acknowledged and minimized, enhancing the credibility and transferability of the findings.

By engaging in continuous and prolonged observation in the field, as referenced in (Bryant, 2007). This helps in developing a comprehensive understanding of the research context and phenomena, increasing the credibility of the findings.

Maintaining a detailed record of the research process, including decisions made, data collection methods, and data analysis procedures, as referenced in (Carias, 2021). This allows for transparency and accountability, thereby enhance the credibility and confirmability of the research.

By providing rich and detailed descriptors of the research context, participants, and data analysis process, as referenced in (Bryant, 2007), (Carias, 2021) This allows readers to assess the credibility and transferability of the findings to other contexts.

3.8.3 *Reliability OR Dependability*

Ensuring consistency in data collection procedures, such as using standardized interview protocols or observation guidelines, as mentioned in references (Bryant, 2007). This helps to minimize variability in data collection and enhances the reliability of the findings.

Maintaining a detailed record of the research process, including decisions made, data collection methods, and data analysis procedures, as referenced in (Bryant, 2007). This allows for transparency and accountability, enabling others to assess the reliability and dependability of the research.

The qualitative insights for this study are drawn from key personnels of SMMEs among them CEOs, CTOs, CIOs, and heads of departments. The study focused on understanding how SMMEs in Gauteng anticipate, detect, withstand, and recover from cyber incidents. To understand the critical success factors employed by the SMME in Gauteng that contribute to cyber resilience of their critical information systems. To get an understanding the best practices that they have in place that demonstrates the cyber resilience of their critical information systems.

Interviews were conducted with CEOs, CTOs, CIOs, and heads of departments of SMMEs. Open-ended questions were used to gather insights of existing cyber security measures that are in place, this was guided by the cyber resilience assessment tool (CR-SAT) framework, which recommends essential domains and policies related to the domains that SMMEs need to have in place to improve their cyber resilience.

Collected data was analysed thematically, data was transcribed, coded, and categorized into themes and sub-themes, that was composed of domains and related policies. The analysis was guided by the research objectives and relevant theoretical frameworks. The trustworthiness of the analysis was ensured through strategies such as prolonged engagement with collected data, and member checking.

Emerging themes and patterns were mapped in the SMME cyber resilience practices of their success factors summarised. The findings were further reviewed to interpret findings and measure of cyber resilience, which is the sum of activities or policies SMMEs action within the domain. For example, in the domain of governance moderated descriptors were used to get the rating of resilience in the domain.

3.8.4 *Generalization*

Generalization refers to the process of extending the findings and conclusions from a specific study to a broader population or context. By generalizing findings researchers can enhance the validity of the study (Bryant, 2007), for example by demonstrating that the identified key dimensions in the CR-SAT framework are

applicable beyond the sampled SMMEs to a larger population of SMMEs in the region. This process ensures that the conclusions drawn from the study are representative and applicable to a broader context, thereby strengthening the validity of the research findings, Morse (2015).

Generalization contributes to the credibility of the study (Bryant, 2007), for example by demonstrating the transferability of identified dimensions in CR-SAT framework to similar SMMEs in Gauteng. Or by showcasing that the findings can be applied to other SMMEs facing similar cybersecurity challenges, the study can gain credibility and relevance in the field of cyber resilience research (Carias, 2021).

In terms of dependability, generalization allows for the replication of the study's findings in different settings or with different samples (Bryant, 2007 of SMMEs in Gauteng. By demonstrating that the key dimensions identified in the CR-SAT framework consistently enhance cyber resilience across various SMMEs, the study's dependability is strengthened, as the results can be reliably replicated in similar contexts, Morse (2015).

Furthermore, generalization contributes to quality assurance in the study by ensuring that the identified dimensions, Morse (2015) for example in the CR-SAT framework are robust and applicable across a diverse range of SMMEs in Gauteng. By generalizing the findings to a broader population, researchers can validate the quality and effectiveness of the framework in enhancing cyber resilience among SMMEs, thereby enhancing the overall quality assurance of the study.

However, there are also challenges associated with generalization these include the potential oversimplification of complex phenomena, the risk of overlooking contextual nuances that may impact the applicability of findings, and the limitations in generalizing findings to populations or contexts that significantly differ from the study sample. The benefits of generalization, however, include the ability to draw broader conclusions, enhance the external validity of the study, and contribute to the advancement of knowledge in the field of cyber resilience among SMMEs in Gauteng

CHAPTER 4. RESULTS

4.1 Introduction

The previous chapter focused on data collection and analysis methodologies of the study. This chapter presents findings from in-depth interviews and analysis of critical success factors influencing cyber resilience among Small, Medium, and Micro Enterprises (SMMEs) in Gauteng. The study engaged with 15 SMMEs for

Attributes of the sample, attributes of SMMEs that were interviewed composed of SMMEs as defined by in The National Small Business in Gauteng. With particular focus to SMMEs that use digital technologies as part of their operational strategy. SMMEs in the health and education sectors were excluded.

The study engaged N=15 SMMEs, however saturation was reached when SMME No7 was interviewed, therefore a decision was taken to stop interviewing at N=8 which was SMME No8. To ensure compliance with relevant legislations and ethics the participants were given codes (SMME No1 to SMME No8) to represent the SMMEs name,

SMME No	Title within the SMME	Brief description of SMME
SMME No1	IT manager	SMME No1 is an organisation in the ICT Sector, based in Midrand, Gauteng region. SMME No1 services to its customers include software development, software integration and business process automation.
SMME No2	CEO	SMME No2 is an organisation in the ICT sector, based in Pretoria. SMME No2 services to its customer include a market platform application, project evaluations and monitoring, assist organisations develop business continuity plans. Its business goal includes assurance of quality of information to enable information-based decision making.
SMME No3	CEO	SMME No3 is based in Fourways area, Johannesburg, Gauteng. It is an investment organisation. Some of its key investment portfolio include investments in telecoms, real estate, financial services organizations. Its main business goal is capital growth.
SMME No4	CEO	SMME No4 is based in Sunninghill, Johannesburg, Gauteng. SMME No4 is an ICT organisation, providing ICT consultancy services to its customers. Some of its services include, Point of Sales solutions, cloud migration, enterprise resource planning and skills training.
SMME No5	IT Executive Consultant	. SMME No5 is an Insurance Broking organisation based on Johannesburg Gauteng. Some of the business goals for the Insurance broking SMME among achieving financial stability includes comply with various legislations including Financial

		Sector Regulation Act (FSRA), Financial Sector Conduct Authority (FSCA) and the POPI Act.
SMME No6	CEO	SMME No6 is based in Sunninghill, Johannesburg, Gauteng. SMME No6 is an ICT organisation, providing ICT consultancy services to its customers. It specialises in dealing with big data, it helps it customers with data design models and drawing insights from data for decision making.
SMME No7	CEO	SMME No7 is based in Soweto, Johannesburg, Gauteng. SMME No7 is an ICT organisation, providing ICT consultancy and advisory services to its customers. It specialises in software development, program management, process optimisation and change management. Its business partner includes CISCO.
SMME No8	A specialist in Development Security and Operations Consultant	A specialist in Development Security and Operations (Dev SEC OPS) consultant based in Johannesburg, Gauteng was interviewed. IT consultant SMME No8 has worked for various SMMEs in the ICT sector. Some of the products and services provided by the SMMEs included software development, cybersecurity services, provisioning of virtual infrastructure, security information and event management.

4.2 Findings

In a digital connectivity with cyber threat landscape and cyber risk that is increasing, the ability of SMMEs to anticipate, detect, withstand, recover from, and evolve after cyber incidents has become a critical area of concern in the economic environment of South Africa.

This study explores the holistic nature of cyber resilience among SMMEs in Gauteng and how the go about ensuring resilience of their critical information systems. To understand the critical success factors and best practices used by these SMMEs to protect their critical information systems. The research aim was to examine the qualitative aspects of cyber resilience to understand the dynamics, obstacles, and innovative ways that shape the cyber resilience of SMMEs.

Given Gauteng's role as a central economic hub, it is crucial to comprehend the qualitative intricacies of cyber resilience among its SMMEs. This understanding is not only academically relevant but also vital for shaping policies, implementing practices, and fostering collaborative initiatives that strengthen the digital defences of these indispensable contributors to the South African economy.

4.3 How do SMMEs in Gauteng anticipate, detect, withstand, and recover from cyber incidents?

To address this research question, this study explored the approaches SMMEs in Gauteng take to cyber resilience of their critical information systems. This was to determine whether their approach to cyber resilience of their critical information systems was proactive of reactive.

The process to gather data was guided by the research questions developed based on the CR-SAT framework for SMMEs. This framework provides a structured approach to operationalizing cyber resilience, enabling organizations to effectively address cyber threats and cyber related risk by addressing shortfalls in the dimension where gaps have been identified. By leveraging the CR-SAT framework, SMMEs in Gauteng can enhance their cybersecurity capabilities and response strategies to combat cyber incidents proactively.

Collected data was analysed by assessing the implementation level and actions that had been taken by the SMME in the policy domain to enhance cybersecurity was assessed using a moderated scale score rating was used as stated in table 2 above and score assigned. For example, in the domain of asset management, implementations codes AM1 which talks policy of SMMEs ability to identify critical assets, as score of zero to five would be assigned depending on the level of capability zero meaning the SMME did not have an inventory list of its critical asset and a score of five meaning the SMME was fully aware and could identify its critical assets. This was repeated for all codes and polices in the domain. This was used to calculate level of implementation in each essential domain, by adding codes AM1, AM2, AM3, AM4 and AM5 of moderated scaled score of policies implemented SMME 1 had an implementation score of 10 in the domain of asset management. The average score for each essential domain was calculated by adding the moderated scaled score of each essential domain for SMME No1 to SMME No8 and dividing it by 8 being the number of SMMEs were involved in the study to establish average level of implementation of each domain among SMMEs, for example in the Asset management domain out of a potential score of 25, SMMEs in Gauteng had a total average implementation score of 18.5 this

helped to understand key dominant cyber resilience success factors employed by SMMEs in Gauteng.

One of the key findings of the study is that SMMEs in Gauteng are increasingly taking proactive approach measures to anticipate potential cyber threats and deal with cyber related risk. This is evidenced by the fact that out of the 8 SMMEs that were interviewed 5 SMMEs have above than average total moderated score in their ability to identify, detect, protect, respond, and recover from cyber threats. These SMMEs demonstrated to have a systematic approach to cyber resilience, this was demonstrated by their ability to have policies, processes, and tools in place that guide their approach to identifying risk associated with their critical information system to risk mitigation, of cyber incidents to withstand and recover from cyber incidents.

Findings reveal that SMMES are adopting a variation of strategies from subscribing to cloud platforms that offer managed security solutions for example Microsoft 365, Symantec, and Kaspersky. These cyber security managed solutions come with comprehensive from endpoint security detection and response, data loss prevention and recovery to providing comprehensive analysis of areas that SMMEs need to address to improve their cybersecurity score. SMMEs are leveraging from high end technology and expertise in cybersecurity skills at affordable prices. Results are presented in table 4 and will be further discussed below.

Table 4: Key Dimensions Result Findings

NIST	Domain	Code	Policy	SMME No1	SMME No2	SMME No3	SMME No4	SMME No5	SMME No6	SMME No7	SMME No8
Identify				25	67	50	71	68	15	20	75
Detect				17	29	19	28	28	6	9	30
Protect				15	15	14	15	15	9	13	15
Respond				12	19	8	15	16	3	6	20
Recover				14	25	15	25	25	9	11	25
Total Modarated Score				**83**	**155**	**106**	**154**	**152**	**42**	**59**	**165**

4.3.1 *Ability to Identify, Detect, Protect, Recover, and Respond*

Results findings for the function to Identify cyber threats was derived from the SMMEs ability to demonstrate performing the recommended essential practices in the domain which included asset management, awareness and training, governance, incident analysis, risk management, threat, and vulnerability management. The SMMEs had to demonstrate capability in the domain through the following: the ability to create and document a baseline configuration for the SMMEs assets. Have a policy in place to manage the changes in the changes in the assets' configurations. Have a policy to periodically maintain the company's assets. Define and document training and awareness plans. Evaluate the gaps in the personnel skills needed to perform their cyber resilience roles and include these gaps in the training plans. Develop and communicate a cyber resilience strategy. Comply with cyber resilience related regulation. Assign resources for example budget, IT personnel, tools to develop cyber resilience activities. Have a process or system in place of lessons learned from previous incidents and implements measures to improve future responses, response and selections, and risk management. They systematically identify and document the SMMEs cyber risks. Classify and prioritize the SMME's cyber risks.

Findings reveal that SMMEs 2,3,4,5 and 8with high moderated score rating demonstrated to have high cyber resilience capabilities towards the NIST function of identifying risk associated with its critical information systems and those with lower moderated score rating SMMEs 1, 6 and 7, did not have a systematic structured approached to cyber resilience had low cyber resilience capability. The above interactive process was repeated for functions Detect, Protect, Respond and Recover Results are represented in table 5 below.

Table 5: Detailed Dimensions Moderated Scale Score Finding**s**

Domain	Code	Policy	SMME No1.	SMME No2.	SMME No3.	SMME No4.	SMME No5.	SMME No6.	SMME No7.	SMME No8.	Av.Score	Key Factors
Asset Management	AM1		2	5	5	5	5	1	2	5	3,75	
	AM2		2	5	5	5	5	1	1	5	3,625	
	AM3		2	5	5	5	5	2	1	5	3,75	
	AM4		2	5	5	5	5	2	1	5	3,75	
	AM5		2	5	5	5	5	1	1	5	3,625	
Asset Management Total			**10**	**25**	**25**	**25**	**25**	**7**	**6**	**25**	**18,5**	**74%**
Awareness and Training	AT1		1	4	5	5	3	2	2	5	3,375	
	AT2		2	4	4	5	4	2	3	5	3,625	
	AT3		5	5	5	5	5	2	4	5	4,5	
	AT4		5	5	5	5	5	5	5	5	5	
Awareness and Training Total			**13**	**18**	**19**	**20**	**17**	**11**	**14**	**20**	**16,5**	**83%**
Business Continuity Managem	BCM1		1	5	1	5	5	1	1	5	3	
	BCM2		2	5	4	5	5	1	1	5	3,5	
	BCM3		3	5	3	5	5	1	1	5	3,5	
Business Continuity Management Total			**6**	**15**	**8**	**15**	**15**	**3**	**3**	**15**	**10**	**67%**
Detection Processes and Cont	DPM1		5	5	5	5	5	5	5	5	5	
	DPM2		1	4	2	5	5	1	1	5	3	
Detection Processes and Continuous Monitoring Total			**6**	**9**	**7**	**10**	**10**	**6**	**6**	**10**	**8**	**80%**
Governance	G1		1	0	1	5	5	0	0	5	2,125	
	G2		1	5	1	5	5	1	1	5	3	
	G3		0	5	3	5	5	0	0	5	2,875	
Governance Total			**2**	**10**	**5**	**15**	**15**	**1**	**1**	**15**	**8**	**60%**
Incident Analysis	IA1		2	5	2	4	4	0	0	5	2,75	
	IA2		2	5	3	4	4	0	1	5	3	
	IA3		2	5	2	5	5	0	2	5	3,25	
	IA4		3	5	1	4	4	0	2	5	3	
Incident Analysis Total			**9**	**20**	**8**	**17**	**17**	**0**	**5**	**20**	**12**	**100%**
Information Security	IS1		5	5	4	5	5	2	4	5	4,375	
	IS2		5	5	5	5	5			5	5	
	IS3		5	5	5	5	5	5	5	5	5	
Information Security Total			**15**	**15**	**14**	**15**	**15**	**7**	**9**	**15**	**14,375**	**53%**
Information sharing and Comr	SHC1		3	5	2	5	5	1	3	5	3,625	
	SHC2		4	5	0	3	4	0	0	5	2,625	
	SHC3		4	4	2	4	4	1	2	5	3,25	
Information sharing and Communication Total			**11**	**14**	**4**	**12**	**13**	**2**	**5**	**15**	**9,5**	**63%**
Risk Management	RM1		1	5	1	5	5	0	0	5	2,75	
	RM2		2	5	2	4	4	1	2	5	3,125	
	RM3		2	5	4	4	4	1	2	5	3,375	
	RM4		2	5	3	4	4	1	2	5	3,25	
Risk Management Total			**7**	**20**	**10**	**17**	**17**	**3**	**6**	**20**	**12,5**	**65%**
Threat and Vulnerability Mana	TVM1		2	4	3	4	4	1	2	5	3,125	
	TVM2		2	5	3	4	4	1	2	5	3,25	
Threat and Vulnerability Management Total			**4**	**9**	**6**	**8**	**8**	**2**	**4**	**10**	**6,375**	**64%**
Total Modarated Score			**83**	**155**	**106**	**154**	**152**	**42**	**59**	**165**	**115,75**	

.

4.4 Which key dimensions of cyber resilience framework do SMMEs in Gauteng implement the different dimensions of cyber resilience?

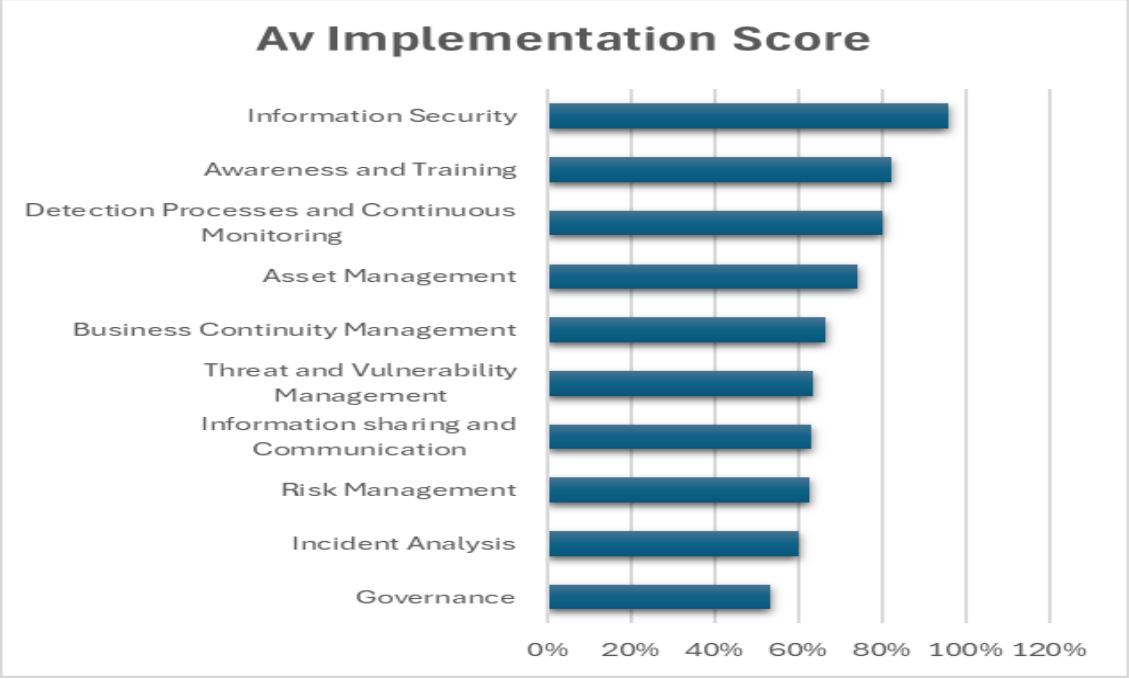
As evidenced and represented in table 5 above SMMEs with high moderated scale score rating had a similarity in that they subscribed to cloud platform solutions with cybersecurity embed features demonstrated to implement all the dimensions of the CR-SAT framework and therefore more cyber resilient while those with low moderated scale score rating have a varied approach implementation of the framework less cyber resilient. For example, SMME No1 has a score of above average on its implementation and procedures in the

domain of training and awareness, risk management, detection and control processes, information sharing and communication, while weak in asset management and governance.

4.5 What are the key success factors or best practices that demonstrate the cyber resilience of critical information systems among SMMEs in Gauteng?

Drawing insights from the Detailed Moderated Scale Score Findings presented in table 5 above it can be concluded based on findings that the key success factors or best practices that demonstrate cyber resilience of the SMMEs' critical information systems are as presented below in figure 3.

Figure 3: Key Dominant Critical Success Factors for SMMEs in Gauteng



The above findings are evidenced further by the fact that despite a varied implementation approach of the CR-SAT all the SMMEs interview had could demonstrate the following:

- Information Management: All the SMMEs could identify their critical information systems or had an understanding on what was critical

information to deliver their goal and objectives. They had implemented some measure of controls like password management, privileged access control, VPN, encryption to safeguard their credentials.

- Training and awareness: all SMMEs demonstrated and saw value in training and awareness and keeping informed about emerging threat landscape, to understand ways of how they can safeguard their critical information or systems. They demonstrated to have some sort of training and awareness in places. This includes internal knowledge sharing sessions, training, communication via email, vendor subscription reports, or following experts on social media platforms.
- Detection process and continuous monitoring: all SMMEs prescribed to a variety of cloud platform services that offered them the capability to identify, detect and mitigate cyber risk these included Microsoft office 365, Amazon web services, antivirus software.

4.6 Conclusion on Findings

Findings of the study demonstrate that SMMEs in Gauteng vary in their approach to cyber resilience, some are proactive in their approach some are reactive. While some SMMEs may prioritize certain dimensions of the CR-SAT framework over others, the overall approach to cyber resilience seems to be characterized by a combination of proactive measures and reactive responses. This finding agrees with Carias *et al.,* (2021) that the CR-SAT can be tailored to the unique challenges faced by SMMEs. It offers a practical and focused approach to assessing cyber resilience, making it more relevant and applicable to SMMEs.

It is evident from the findings that SMMEs do not systematically employ all dimensions of the CR-SAT framework. And the key dominant critical success factors that are key to cyber resilience of SMMEs in Gauteng in order of the highest top three rankings are information security, training, and awareness, and detecting processes and continuous monitoring.

.

CHAPTER 5. CONCLUSION AND RECOMMENDATION

5.1 Introduction

This study explores the holistic nature of cyber resilience among SMMEs in Gauteng and how they go about ensuring resilience of their critical information systems. The aim was to understand the approach to cyber resilience that is exhibited in SMMEs. To understand the key dimensions as recommend in the CR-SAT theoretical framework that SMMEs in Gauteng employ. To understand key critical success factors and best practices employed by SMMEs in Gauteng to protect their critical information systems. The research aim was to explore the qualitative aspects to draw deeper meaningful insights of the dynamics, obstacles, and innovative ways that shape the cyber resilience of SMMEs.

The approach for this study was as follows, chapter 1 of this study introduced the research problem and gave context of the challenges that SMMEs face in a digital environment where cyber threats and associated risk are constantly increasing. Chapter 2 explored literature and conducted a literature review to find out ways how SMMEs can improve cyber security, cyber resilience. Chapter 3 looked at the methodology in how the research would be conducted, looking at how the researcher would go about drawing insights from SMMEs to answer the research questions. It looked at ways how analysis drawn from insight would be presented as findings free from bias of the researcher but representing true insights from the SMMEs. Chapter 4 presented the findings of the study. And this chapter will interpret the findings within the context of literature review.

5.2 Measuring cyber resilience using the moderated scale score rating

As highlighted in Kott & Linkov (2021) and (Linkov & Kott, 2019), measuring cyber resilience is a complex task. There is a lack of rigorous and qualitative methods to measure cyber resilience implementations outcomes. The meaning of cyber resilience, the term itself is often misunderstood. Traditional risk

assessment approaches may not adequately account for the interdependencies and cascading effects in complex and interconnected systems.

Determining the moderated score rating based on details a reflected in table 2 above to assign to the policy in the essential dimension of measure proved to challenge and subjective.

5.3 How do SMMEs Approach Cyber Resilience

The goal was to understand how SMMEs in Gauteng approach cyber resilience, to understand the good practices and critical success factors that SMMEs employ that enhance cyber resilience. To explore if SMMEs employ all the essential dimensions as recommended by CR-SAT framework, which have their foundation from the NIST framework.

The study by Linkov & Kott, (2019) highlights the importance of cyber resilience in a society that is increasingly being reliant upon complex and interconnected cyber systems to conduct daily activities, and the adverse loss that can be happen because of cyber incidents. Highlighting the need for SMMEs to have the ability to anticipate, detect, withstand, recover, and evolve from cyber incidents to enhance resilience.

Studies by Carias, et al. (2021) emphasizes that self-assessment by SMME using the CR-SAT framework can highlight areas that an SMME may need to address to improve its overall abilities recover and evolve from cyber incidents to enhance resilience emphasizes self-assessment, enabling the SMME to evaluate their cyber resilience capabilities independently. This self-assessment empowers the SMME to identify areas of improvement, and by addressing the areas of improvement the SMME can take proactive measures to enhance their cyber resilience Carias, et al. (2021).

Findings drawn from the insights of SMMEs in Gauteng found that SMMEs that employed all the essential dimensions of the CR-SAT theoretical framework demonstrated proactive abilities to anticipate, withstand, recover, and evolve from cyber incidents.

This therefore confirms that SMMEs that embed systemically the essential dimensions of the CR-SAT framework are better poised to withstand and evolve from cyber incidents.

5.4 Do SMMEs in Gauteng employ all the dimensions of the CR-SAT framework.

Literature reviewed showed that if SMMEs employed baseline essential practices domains that are key to achieve cyber resilience, this included critical success factors as recommended by The South African Reserve Bank Prudential Authority and the Financial Sector Conduct Authority, Authority, (2022). The Carnegie Mellon University Software Engineering Institute, Matt Trevors & Wallen, (2017) which proposes the CERT Resilience Management Model (CERT-RMM) which comprises of 11 baseline practice areas. Various academic research papers, and CR-SAT conceptual framework which proposed similar success factors that can enhance the overall cyber resilience of SMMEs.

Findings of the study indicate that while some SMMEs in Gauteng demonstrate a varied approach to implementation of CR-SAT recommended essential domains, data insights revealed that SMMEs that demonstrated a more proactive approach to cyber resilience also demonstrated a stronger ability to detect, protect, withstand and evolve from cyber incidents. Those that had a reactive approach demonstrated less ability to withstand and evolve from cyber incidents.

This therefore further agrees with the literature review evidence that employing all the essential dimensions of CR-SAT is key to achieving cyber resilience and therefore minimise cyber related risk for SMMEs.

5.5 What are key critical success factors for SMME in Gauteng

Literature highlighted training and awareness, risk management and Incident response and business continuity to be key dominant factors for the SMME should aim towards achieving. Carias, (2020), Walaza et al., (2020), (Cilliers &

Chinyamurindi, 2020), (Kelly et al., 2022) highlights that employee awareness and training in enhancing cyber resilience for SMMEs. The study emphasizes the need for conducting the SMMEs cyber skills analysis, educating employees about cyber threats, safe online practices, and the importance of reporting incidents. Regular training sessions can help create a security-conscious culture within the organization.

There is still room for improvement in terms of employing all dimensions of the CR-SAT framework. Especially in governance. The study found that many SMMEs focus primarily on risk management and incident management, while systematic approach in the dimensions of governance, stakeholder engagement is addressed in an ad hoc manner.

Key critical success factors that influence the cyber resilience of critical information systems exhibited in the SMMEs include the adoption of best practices in cybersecurity, regular assessment of risks and vulnerabilities, the implementation of incident response plans, and ongoing training and awareness initiatives for employees, outsourcing, dealing with credible vendors.

5.6 Conclusion and recommendations

Overall, the findings of the study highlight the need for SMMEs in Gauteng to consider systematically implementing all dimensions of the CR-SAT framework and to prioritize key critical success factors to effectively enhance their cyber resilience. By doing so, SMMEs can better protect their critical information systems and mitigate the risks associated with cyber threats.

REFERENCES

Africa, R. o. S. (1996). *National Small Business Act No 102, 1996*. Retrieved from https://www.gov.za/documents/national-small-business-act#:~:text=The%20National%20Small%20Business%20Act,provide%20for%20matters%20incidental%20thereto.

Agupusi, P. (2007). Small BusinessEntrepreneurship DevelopmentSocial Entrepreneurship. *JOUR*.

Aliyu, A., et al. (2015). ONTOLOGY, EPISTEMOLOGY AND AXIOLOGY IN QUANTITATIVE AND QUALITATIVE RESEARCH: ELUCIDATION OF THE RESEARCH PHILOSOPHICAL MISCONCEPTION. The Academic Conference: Mediterranean Publications & Research International on New Direction and Uncommon, University of Agric, Abekuta, Abekuta, Ogun State, Nigeria.

Authority, F. S. C. A. a. S. A. R. B. P. (2022). Draft Joint Standard – Cybersecurity and cyber resilience requirements for financial institutions. In.

Bhorat, H., et al. (2018). SMMES in South Africa: Understanding the Constraints on Growth and Performance. *Communications Manager: Development Policy Research Unit*.

Björck, F., et al. (2015). Cyber Resilience – Fundamentals for a Definition. In A. Rocha, A. M. Correia, S. Costanzo, & L. P. Reis, *New Contributions in Information Systems and Technologies* Cham.

Burns, N., et al. (2005). *Selecting a quantitative research design. Burns N, Grove SK (eds), The Practice of Nursing Research: Conduct, Critique, and Utilization* (5th edition. ed.).

Bvuma, S., & Marnewick, C. (2020). Sustainable Livelihoods of Township Small, Medium and Micro Enterprises towards Growth and Development. *Sustainability*, *12*(8), 3149. https://doi.org/10.3390/su12083149

Cahyono, E. B., et al. (2022). A review on cyber resilience model in small and medium enterprise. *Paper presented at the 4th International Conference on Smart Sensors and Application: Digitalization for Societal Well-being, ICSSA Kuala Lumpur, Malaysia, 2022*, 114-119. https://doi.org/10.1109/ICSSA54161.2022.9870952

Caitlyn Murphy, et al. (2022). Factors Affecting Compliance with the National Cybersecurity Policy by SMMEs in South Africa. The 8th Annual ACIST Proceedings,

Cant, M. (2003). *Marketing research,* .

Caralli, R. A., et al. (2010). CERT®

Resilience Management Model,

Version 1.0. *CERT Program*. http:// www.cert.org/resilience/

Caralli, R. A., et al. (2012). Maturity Models 101: A Primer for Applying Maturity Models to Smart Grid Security, Resilience, and Interoperability.

Carias, J. F., et al. (2021). Cyber Resilience Self-Assessment Tool (CR-SAT) for SMEs. *IEEE Access 9*, *80741-80762*. https://doi.org/https://doi.org/10.1109/access.2021.3085530

Carías, J. F., et al. (2020). Systematic Approach to Cyber Resilience Operationalization in SMEs. *IEEE Access 8*, *174200–174221*. https://doi.org/https://doi.org/10.1109/access.2020.3026063

Carpenter, M. H., et al. (2014). Entropy Stable Spectral Collocation Schemes for the Navier--Stokes Equations: Discontinuous Interfaces. *SIAM Journal on Scientific Computing*, *36*(5), B835-B867. https://doi.org/10.1137/130932193

Chatterjee, M. B. D. (2020). Calculated risk? A cybersecurity evaluation tool for SMEs. *Business Horizons*, 531-240.

Cheung, V. (2017). The importance of SMMEs on the South African economy. *TOPCO BULLETIN*. https://topperforming.co.za/the-importance-of-smmes-on-the-south-african-economy/

Cilliers, L., & Chinyamurindi, W. (2020). Perceptions of cyber bullying in primary and secondary schools among student teachers in the Eastern Cape Province of South Africa. *The Electronic Journal of Information Systems in Developing Countries*, *86*(4). https://doi.org/10.1002/isd2.12131

Cohen, L., et al. (2017). *Research Methods in Education*. https://doi.org/https://doi.org/10.4324/9781315456539

Collinson, et al. (2011). *The Sage Handbook of Leadership*.

Crane, C. (2021). *5 Small Business Cyber Security Statistics That You*

Need to Know. https://www.thesslstore.com/blog/15-small-business-cyber-security-statistics-that-you-need-to-know/

Creswell, J. (2013). Steps in Conducting a Scholarly Mixed Methods Study.

Creswell, J., et al. (2003). Advance Mixed methods Research Designs. In (pp. 209-240).

Crotty, M. (1998). The foundations of social research. https://doi.org/10.4324/9781003115700

Denzin, N. K. (2010). Moments, Mixed Methods, and Paradigm Dialogs. *Qualitative Inquiry*, *16*(6), 419-427. https://doi.org/10.1177/1077800410364608

Dupont, B. (2019). The cyber-resilience of financial institutions: significance and applicability. *Journal of Cybersecurity*, *5*(1). https://doi.org/10.1093/cybsec/tyz013

Durrheim, K. (1996). Book Review: Handbook of Qualitative Research. *South African Journal of Psychology*, *26*(4), 257-258. https://doi.org/10.1177/008124639602600410

Gabriel, A. J., et al. (2021). *Cyber Security in the Age of COVID-19. In: Hassanien, A.E., Darwish, A. Digital Transformation and Emerging Technologies for Fighting COVID-19 Pandemic: Innovative Approaches. Studies in Systems, Decision and Control* (Vol. 322). https://doi.org/https://0-doi-org.innopac.wits.ac.za/10.1007/978-3-030-63307-3_18

Ghauri, P., & Grønhaug, K. (2005). Research Methods in Business Studies: A Practical Guide.

Groenendaal, J., & Helsloot, I. (2021). Cyber resilience during the COVID-19 pandemic crisis: A case study. *Journal of Contingencies and Crisis Management*, *29*(4), 439-444. https://doi.org/10.1111/1468-5973.12360

Guba, E. G., et al. (2005). Paradigmatic Controversies, Contradictions, and Emerging Confluences. In *The Sage handbook of qualitative research, 3rd ed.* (pp. 191-215). Sage Publications Ltd.

Hills, M., & Atkinson, L. (2016). *Why Cyber Security is a Socio-Technical Challenge: New Concepts and Practical Measures to Enhance Detection, Prevention and Response :* (M. Hills, Ed.). Nova Science Publishers. https://doi.org/http://nectar.northampton.ac.uk/id/eprint/8683

IBM. (2022). *Cost of a Data Breach Report for 2022* (IBM Security, Issue. https://www.ibm.com/downloads/cas/3R8N1DZJ

Idi Mohammed, & Bade, A. M. (2019). CYBERSECURITY CAPABILITY MATURITY MODEL FOR NETWORK SYSTEM. *International Journal of Development Research*, *09*(07), 28637-28641. http://www.journalijdr.com/

Institute, P. M. (2021). *A Guide to the Project Management body of knowledge and The Standard for Project Management* (7th ed.). Project Management Institute.

Johnson, J. L., et al. (2020). A Review of the Quality Indicators of Rigor in Qualitative Research. *American Journal of Pharmaceutical Education*, *84*(1), 7120. https://doi.org/10.5688/ajpe7120

Jovanovic, B. (2024). A Not-So-Common Cold: Malware Statistics in 2024. Retrieved 2024/02/28, from https://dataprot.net/statistics/malware-statistics/

Kelly, A. D., et al. (2022). AN EVALUATION OF GOVERNMENT SUPPORT SERVICES FOR SMMEs IN THOHOYANDOU, SOUTH AFRICA. *Journal of Entrepreneurial Innovations*, *2*(1). https://doi.org/10.14426/jei.v2i1.1163

Kortjan, N. and Solms, R. v. (2014). A conceptual framework for cyber security awareness and education in sa. South African Computer Journal, 52. https://doi.org/10.18489/sacj.v52i0.201

Kott, A., & Linkov, I. (2021). To Improve Cyber Resilience, Measure It. *Computer*, *54*(2), 80-85. https://doi.org/10.1109/mc.2020.3038411

Lang, K. R., & Li, T. (2013). Introduction to the Special Issue: Business Value Creation Enabled by Social Technology. *International Journal of Electronic Commerce*, *18*(2), 5-10. https://doi.org/10.2753/jec1086-4415180200

Linkov, I., & Kott, A. (2019). Fundamental Concepts of Cyber Resilience: Introduction and Overview. In *Cyber Resilience of Systems and Networks* (pp. 1-25). Springer International Publishing. https://doi.org/10.1007/978-3-319-77492-3_1

Loonam, J., et al. (2022). Cyber-Resiliency for Digital Enterprises: A Strategic Leadership Perspective. *IEEE Transactions on Engineering Management*, *69*(6), 3757-3770. https://doi.org/10.1109/tem.2020.2996175

Madondo, S. M. (2021). Data Analysis and Methods of Qualitative Research: Emerging Research and Opportunities. In (pp. 249). https://doi.org/10.4018/978-1-7998-8549-8

Malatji, M., et al. (2020). Cybersecurity Policy and the Legislative Context of the Water and Wastewater Sector in South Africa. *Sustainability*, *13*(1), 291. https://doi.org/10.3390/su13010291

Malhotra, N., et al. (2007). *Marketing Research: an applied approach: 3rd European Edition*.

Malhotra, N. K. (2010). *Marketing Research: An Applied Orientation*. Pearson Education. https://books.google.co.za/books?id=VLwVPwAACAAJ

Malhotra, N. K. (2013). *Basic Marketing Research: Pearson New International Edition*. Pearson Education. https://books.google.co.za/books?id=sAmpBwAAQBAJ

Malhotra, N. K., & M, P. (2012). *Basic marketing research. New Jersey: Pearson.* .

Marsh. (2021). The Changing Face of Cyber Claims.

Matt Trevors, & Wallen, C. M. (2017). *Cyber Hygiene: A Baseline Set of Practices*

Mbanaso, U. M., et al. (2019a). Conceptual Design of a Cybersecurity Resilience Maturity Measurement (CRMM) Framework. *The African Journal of*

Information and Communication (AJIC)(23), 1–26. https://doi.org/https://doi.org/10.23962/10539/27535

Mbanaso, U. M., et al. (2019b). Conceptual design of a Cybersecurity Resilience Maturity Measurement (CRMM) Framework. *The African Journal of Information and Communication*, *2019*(23), 1-26. https://doi.org/doi:10.23962/10539/27535

Mehravar, N. (2013). *Resilience Management through Use of CERT-RMM*

& Associated Success Stories 2013 IEEE International Conference on Technologies for Homeland Security (HST), Waltham, MA, USA.

Mertens, D. (2006). Book Review: Research and Evaluation in Education and Psychology: Integrating Diversity With Quantitative, Qualitative, and Mixed Methods (2nd ed.). *American Journal of Evaluation*, *27*(3), 399-401. https://doi.org/10.1177/1098214006291009

Mitchell, et al. (2010). *Research design explained: Instructor's edition, 7th ed*. Wadsworth/Cengage Learning.

NIST, N. I. o. S. a. T. (2014). Framework for Improving Critical Infrastructure Cybersecurity. In. https://www.nist.gov/system/files/documents/cyberframework/cybersecurity-framework-021214.pdf: NIST.

NIST, N. I. o. S. a. T. (2018). Framework for Improving Critical Infrastructure Cybersecurity. In.

Omera Khan, D. A., & Sepúlveda Estay. (2015). Supply Chain Cyber-Resilience: Creating an Agenda for Future Research. *Technology Innovation Management Review*, *5*(4). http://timreview.ca/article/885

Radanliev, P., et al. (2019). *Cyber Risk impact Assessment - Assessing the Risk from the IoT to the Digital Economy*. MDPI AG.

Robert Johnson, I. (2019, Jan. 2, 2019). 60 Percent Of Small Companies Close Within 6 Months Of Being Hacked. *Cybercrime*. https://cybersecurityventures.com/60-percent-of-small-companies-close-within-6-months-of-being-hacked/

Robert P. Hartwig, & Claire, W. (2013). Cyber Risks: The Growing Threat. *Insurance Information Insitute*. https://www.iii.org/sites/default/files/paper_CyberRisk_2013.pdf

Rungani, et al. (2018). The impact of financial support on the success of small, medium and micro enterprises in the Eastern Cape province. *Acta Commercii*, *18*(1). https://doi.org/10.4102/ac.v18i1.591

Salah Kabanda, et al. (2018,). Exploring SME cybersecurity practices in developing countries. *JOURNAL OF ORGANIZATIONAL COMPUTING*

AND ELECTRONIC COMMERCE, *VOL. 28,*(NO. 3,), 269–282. https://doi.org/https://doi.org/10.1080/10919392.2018.1484598

Saunders, M., et al. (2019). "Research Methods for Business Students" Chapter 4: Understanding research philosophy and approaches to theory development. In (pp. 128-171).

Schulze, et al. (2014). The use of mixed methods as reflected in two eminent South African educational research journals. *Journal for New Generation Sciences*, *10*(1), 130 -147. https://doi.org/https://journals.co.za/doi/pdf/10.10520/EJC126830

Scotland, J. (2012). Exploring the Philosophical Underpinnings of Research: Relating Ontology and Epistemology to the Methodology and Methods of the Scientific, Interpretive, and Critical Research Paradigms. *English Language Teaching*, *5*(9). https://doi.org/10.5539/elt.v5n9p9

Sharkov, G. (2020). Assessing the Maturity of National Cybersecurity and Resilience. *The Quarterly Journal,*, *19*(4). https://doi.org/https://doi.org/10.11610/Connections.19.4.01

Solms, B. v. (2019). CYBER SECURITY BEST PRACTICES FOR SMES. In. https://smesouthafrica.co.za/cyber-security-best-practices-for-smes/: SME South Africa.

Stats_SA. (2022). *Stats in brief. improving lives through data ecosystems*. Retrieved from https://www.statssa.gov.za/publications/StatsInBrief/StatsInBrief2022.pdf

Symonds, J. E., & Gorard, S. (2010). Death of mixed methods? Or the rebirth of research as a craft. *Evaluation & Research in Education*, *23*(2), 121-136. https://doi.org/10.1080/09500790.2010.483514

Tierney, A. J. (2002). Research design in social research: David de Vaus; SAGE Publications Ltd., London, California, New Delhi, 2001, ISBN 0-7619-5347-7. *International Journal of Nursing Studies*, *39*(6), 669-670. https://doi.org/https://doi.org/10.1016/S0020-7489(01)00040-2

Trim, P., & Lee, Y.-I. (2004). Enhancing customer service and organizational learning through qualitative research. *Qualitative Market Research: An International Journal*, *7*, 284-292. https://doi.org/10.1108/13522750410557094

Umunnakwe, A., et al. (2021). Cyber-physical component ranking for risk sensitivity analysis using betweenness centrality. *IET Cyber-Physical Systems: Theory & Applications*, *6*(3), 139-150. https://doi.org/10.1049/cps2.12010

Vuba, S. (2019). The missed opportunity: SMMEs in the South African economy. Retrieved 2024/01/28, from

Walther, J., et al. (2013). Quality in Interpretive Engineering Education Research: Reflections on an Example Study. *Journal of Engineering Education*, *102*(4), 626-659. https://doi.org/https://doi.org/10.1002/jee.20029

Williams, P. A. H., & Manheke, R. J. (2010). Small Business - A Cyber Resilience Vulnerability.

Zwass, V. (2010). Co-Creation: Toward a Taxonomy and an Integrated Research Perspective. *International Journal of Electronic Commerce*, *15*(1), 11-48. https://doi.org/10.2753/jec1086-4415150101

APPENDIX A – Research Instrument

Name of SMME:

Interviewing: Key responsible person in the SMME (CTO's CIO's CEO's)

Introduction: These interview questions are designed to gather insights into the critical success factors and best practices related to cyber resilience.

Research instrument interview questions.

1. Can you briefly describe your organization's approach to cyber resilience and its importance in the context of your operations?
2. In your experience, what are the critical success factors that contribute to effective cyber resilience in organizations?
3. How does leadership support and commitment influence the cyber resilience of your organization?
4. What role does employee awareness and training play in enhancing cyber resilience? Can you provide examples of effective training programs or initiatives?
5. How do you ensure that your organization has the necessary cybersecurity measures in place to protect against cyber threats? What best practices do you employ?
6. Can you share any experiences or examples where your organization successfully recovered from a cyber-attack? What factors contributed to the resilience demonstrated in those situations?
7. How do you assess and manage the risks associated with cyber threats? Are there any specific risk assessment methodologies or frameworks that you find effective?
8. What role does collaboration and information sharing with external stakeholders (e.g., industry peers, government agencies, cybersecurity experts) play in enhancing cyber resilience?
9. How do you ensure that your organization stays updated with the latest cybersecurity trends and technologies? Are there any specific resources or strategies that you find helpful in this regard?

10. Can you share any lessons learned or recommendations for other organizations looking to enhance their cyber resilience? What advice would you give to them?

APPENDIX B – Participant Information

Example of a Participant Information Sheet (PIS), NB this is NOT a template.

Wits letterhead (optional)

Dear Sir / Madam or Good day or (similar)

My name is XXXX. I am a Masters/PhD student/staff member in XXXXX at the University of the Witwatersrand, Johannesburg. My supervisor is Dr / Prof. XXXXX. I am conducting a research study about XXXXX. The study title is XXXXX.

I am inviting you to take part in an interview/focus group/answer a questionnaire/XXXXX. If you decide to take part, your participation in this research study will last about XXXXX. The interview/research activity will take place at [this place] at [this time].

With your permission, I would like to audio/video record the interview/focus group. This data will be stored in XXXXX for XXX years and/or deleted after XXX years. Only the researcher will have access to the data.

During the research activity, I will need to ask for some personal information about you, including XXXXX

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

If you decide to take part in the research study, it should be because you want to volunteer. You do not have to take part. You can stop being in the study at any time. You do not have to answer any questions if you do not want to. You will not get any direct benefits if you choose to join the research study. You will not lose any services, benefits, or rights you would normally have if you decide not to join. Taking part in the research study will not cost you anything. You will not be paid for being in this research study. Your travel/data costs to attend the interview/XXXX will be reimbursed to a maximum of R150.

The risks for this research study are no more than what happens in everyday life. OR Some of the questions asked may make you feel sad or upset. If this happens, I will stop the interview/XXXX and continue another time. If you need support or counselling services following the interview/XXXX, these are available free of charge at XXXX. The name of the counsellor is XXXX and the contact details for the counselling service are XXXX.

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

If you have any questions during or afterwards about this research study, feel free to contact me or my supervisor on the details listed below. If you have any concerns or

complaints about the ethical procedures of this research study, you are welcome to contact the University Human Research Ethics Committee (Non-Medical), telephone +27(0) 11 717 1408, email hrecnon-medical@wits.ac.za.

Yours sincerely,

XXXX

Researcher:

Your full name, Wits email, your phone number

Supervisor:

Their full name, Wits email, Wits phone number

APPENDIX C – Participant Consent Form

Investigating cyber resilience in Small, Medium, and Micro Enterprises (SMME's) in Gauteng

Consent to take part in research.

- I…… voluntarily agree to participate in this research study.
- I understand that even if I agree to participate now, I can withdraw at any time or refuse to answer.
- any question without any consequences of any kind.
- I understand that I can withdraw permission to use data from my interview within two weeks after
- the interview, in which case the material will be deleted.
- I have had the purpose and nature of the study explained to me in writing and I have had the
- opportunity to ask questions about the study.
- I understand that participation involves *critical success factors in terms of policies and procedure that the SMME employs as strategies to address cybersecurity measures. To ensure that critical information systems are protected and the SMME continues to operate after cyber threat events*.
- I understand that I will not benefit directly from participating in this research.
- I agree to my interview being audio-recorded.
- I understand that all information I provide for this study will be treated confidentially.
- I understand that in any report on the results of this research my identity will remain anonymous.
- This will be done by changing my name and disguising any details of my interview which may reveal my identity or the identity of people I speak about.
- I understand that disguised extracts from my interview may be quoted in final research report on that you plan to use the data.
- I understand that if I inform the researcher that myself or someone else is at risk of harm, they may have to report this to the relevant authorities - they will discuss this with me first but may be required to report with or without my permission.
- I understand that signed consent forms and original audio recordings will be retained in accordance with POPI(Act) for 5 years in an online database,
  With secure multi-password access authentication after students this will be until the exam board confirms the results of their dissertation.

- I understand that a transcript of my interview in which all identifying information has been removed will be retained for – for students this will be 5 years from the date of the exam board.
- I understand that under freedom of information legalisation I am entitled to access the
- information I have provided at any time while it is in storage as specified above.
- I understand that I am free to contact any of the people involved in the research to seek further.

Edna Kamanga, 2417875@Students.wits.ac.za Supervisor: (DR Kiru Pillay).

Signature of research participant

---------- ----------

Signature of participant Date

Signature of researcher

I believe the participant is giving informed consent to participate in this study.

---------- ----------

Signature of researcher Date:

APPENDIX D – Signed Non-Disclosure Agreement

CONFIDENTIALITY AGREEMENT

THIS AGREEMENT is made on.

PARTIES

XXXXXXXX and Company/SMME/XXXX a Legal Person in terms of the Law of South Africa with registration number XXXXXX with Principal Place of Business at XXXXX Street, Johannesburg, Gauteng, and includes all entities within the South Africa.

And

XXXXXX, a recognised as an adult in terms of the Laws of South Africa with DOB/ID number XXXX and principal place of business at XXXX, XXXX, XXXXXXX Centre, XXX Dr, Midrand.

BACKGROUND

The Disclosing Party wishes to disclose to the Recipient and wishes to ensure that the Recipient maintains the confidentiality of the Disclosing Party's Confidential Information. In consideration of the benefits to the parties of disclosing and receiving the Confidential Information, the parties have agreed to comply with the following terms in connection with the use and disclosure of Confidential Information.

AGREED TERMS

DEFINITIONS AND INTERPRETATION

The following definitions and rules of interpretation in this clause apply in this Agreement:

"Business Day" means a day (other than a Saturday, Sunday, or public holiday) when the banks in South Africa are open for business.

"Confidential Information" means all confidential information (however recorded or preserved) disclosed or made available, directly, or indirectly, by the Disclosing Party or its employees, officers, representatives, or advisers to the Recipient including but not limited to:

the fact that discussions and negotiations are taking place concerning the Purpose and the status of those discussions and negotiations.

the existence and terms of this Agreement.

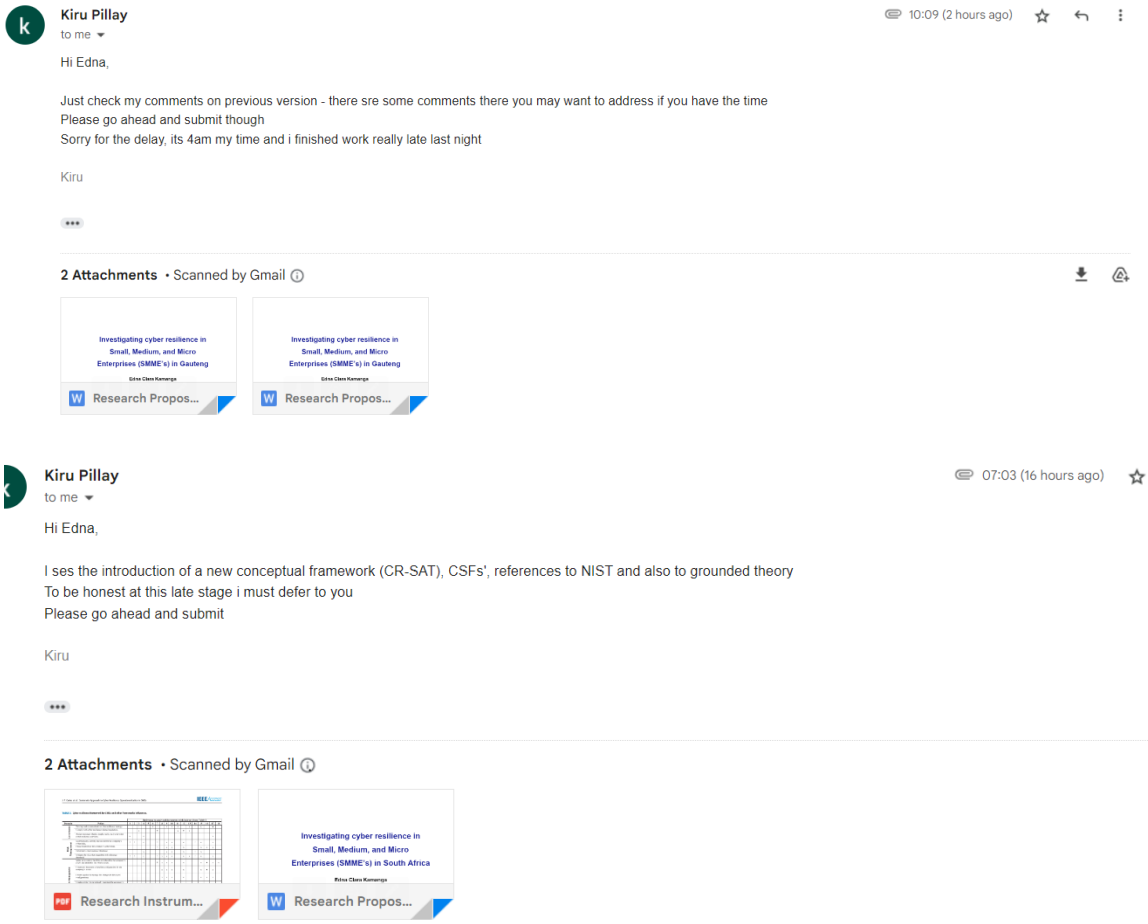
any information that would be regarded as confidential by a reasonable businessperson relating to:

the financial statements, business, affairs, customers, clients, suppliers, plans, intentions, or market opportunities of the Disclosing Party or of the Disclosing Party's Group, and

the operations, processes, product information, know-how, intellectual property, designs, trade secrets or software of the Disclosing Party or of the Disclosing Party's Group; and

any information or analysis derived from the Confidential Information.

APPENDIX E – Supervisor Email



Kiru Pillay
to me

10:09 (2 hours ago)

Hi Edna,

Just check my comments on previous version - there sre some comments there you may want to address if you have the time
Please go ahead and submit though
Sorry for the delay, its 4am my time and i finished work really late last night

Kiru

2 Attachments • Scanned by Gmail

Investigating cyber resilience in Small, Medium, and Micro Enterprises (SMME's) in Gauteng
Edna Clara Kamanga
Research Propos...

Investigating cyber resilience in Small, Medium, and Micro Enterprises (SMME's) in Gauteng
Edna Clara Kamanga
Research Propos...

Kiru Pillay
to me

07:03 (16 hours ago)

Hi Edna,

I ses the introduction of a new conceptual framework (CR-SAT), CSFs', references to NIST and also to grounded theory
To be honest at this late stage i must defer to you
Please go ahead and submit

Kiru

2 Attachments • Scanned by Gmail

Research Instrum...

Investigating cyber resilience in Small, Medium, and Micro Enterprises (SMME's) in South Africa
Edna Clara Kamanga
Research Propos...

APPENDIX F – Ethics Clearance Certificate

Graduate School of Business Administration
University of the Witwatersrand, Johannesburg

Wits Business School

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

Ethics Clearance Certificate

Ethics protocol number: WBS/DB2417875/864
This certificate is only valid with a legitimate ethics protocol number and signed by the Researcher (below).

Project title	Investigating cyber resilience in small, medium, micro enterprises (SMMEs) in Gauteng
Investigator / Researcher	Ms Edna Kamanga
Nature of Project	MM (Digital Business)
Decision of the Committee	Approved, provided stakeholders and participants are guaranteed confidentialty.
Issue Date of Certificate	2023/10/13
Expiry date	Date of submission of the project / research report
Chairperson	Dr Pius Oba +27 11 717 3976 +27 82 733 6587 pius.oba@wits.ac.za

Declaration by Researcher

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

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

Signature

2023/10/17
Date: